Component	Service	Protocol	Port	Description
			1025-65535	

J.10.6 Ports – DiskXtender

J.10.6.1 Ports used by DX-NAS

Port number	Description
139	NetApp callback (not configurable) **Note:** If DX-NAS is used to migrate files from a NetApp filer, you cannot run Samba on the same machine where the DX-NAS server is running.
445	CIFS
2049	NFS
1976	DX-NAS database
3682	• EMC Centera CLI • EMC Centera Viewer • EMC Centera communication
8080	DX-NAS web server
[redacted] b7E	DX-NAS server (configurable)

Department of Justice

Federal Bureau of Investigation

INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (IAFIS)

INTERFACE CONTROL DOCUMENT (ICD)

September 3, 2008

IAFIS-DOC-05125-25.0

Prepared By:

Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road Clarksburg, WV 26306

NGI-2

CHANGE HISTORY

A. IAFIS-IC-0020, February 1, 1993; Baseline Version

B. IAFIS-IC-0020 (V1), September 1, 1993—This version adds IOC data flows as Appendix D, updates FOC data flows in Appendix B, makes modifications to message definitions in Appendix A, updates text in IAFIS Functional Interfaces section and the IAFIS Communications Interfaces section to reflect above mentioned modifications, and makes other minor adjustments. The CCB approved RFCs incorporated in version one (V1) are 126, 146, 160, 162, 171, 173, 177, 178, 179, 180, 181, 182, 183, 184, 185, 292, 294, and 295.

C. IAFIS-IC-0020 (V2), August 17, 1994—This version updates the IOC and FOC data flows to reflect the message name and numbers appearing in the Message Definition Database (MDD). It also provides a new Appendix A, IAFIS Message Definitions, which presents the use of the MDD for configuration control of the messages. This version also removes all references to configuration management as a MIDS function, changes the transaction ownership for Electronic Consolidations, incorporates data flows for CCNR Modifications, III File Maintenance Requests, and III Inquiries, and makes other minor adjustments. The CCB approved RFCs incorporated in version two (V2) are 464(R1), 602, 604, 631, 649, 650, 660, 661, 665, 670, 689, 690, 691, 696, 697, and 709.

D. IAFIS-IC-0020 (V3), March 21, 1995—This version updates the IOC and FOC data flows, and sections 3 and 4 of the basic document to reflect technical changes resulting from an extensive Critical Requirements Issues Working Group effort. In addition to general changes to the data flows, specific clarification concerning communication interfaces, the IN/FICS interface, procedures for restoring criminal data, civil processing, record consolidation, MIDS definition, and some aspects of Latent processing were changed. The E/F CCB-approved RFCs incorporated in version 3 (V3) are 782, 807, 808, 809, 810, 811, 812, 820, 840, 841, and 863.

E. IAFIS-IC-0020(V4) August 18, 1995—This version updates the ICD with RFCs 902 and 821. RFC 902 contained numerous administrative updates discovered during a review of V3. RFC 821 documents the concepts of Transaction Handshaking and File Synchronization within IAFIS.

F. IAFIS-IC-0020(V5) November 2, 1995. This version incorporates new data flows added in RFC 901, includes III/FBI segments resolutions identified in RFC 915 and the administrative RFC 928. In addition to these RFCs, the following corrections were incorporated:
"FCE has been globally changed to "FE."
"(RFC)" has been changed to "RFC."
ITN, AFIS, and III have been changed to IN/FBI, AFIS/FBI and III/FBI.
"TBR" has been changed to "TBD."
All references to the Electronic Fingerprint Transmission Specification (EFTS) have been standardized.

G. IAFIS-IC-0020(V6), December 14, 1995—This version incorporates RFC 909, which

eliminated all direct and indirect electronic communication between LCMS and IAFIS; RFC 921 removes Table 6-2, updates Table 3-1, Table 12, Table 13 and Table 14, numerous messages in Sequencing and Notes, miscellaneous updates to Figures, and various administrative updates; and RFC 934, which completes the contents of the Message Definition Database and is included in Appendix A. It also reflects refinements in file maintenance operations (Appendices B and D) and further definition of latent fingerprint processing (Appendix B).

H. IAFIS-IC-0020(V7), September 12, 1996—This version incorporates RFC 897 (V6R1), which modifies IAFIS ICD to add new message information to Tables 3-1, adds new IOC and FOC data Flow diagrams, and provides MDD message information; RFC 904 (V6R1), to clarify the file comparison requirements in the III/FBI, AFIS/FBI, and IN/FBI Segment Specifications; RFC 917 (V6R1), allows DPS service providers to request RANRs or other reports; RFC 924 (V6R1), which updates reference to Electronic Fingerprint Transmission Specification (EFTS) version 4 dated August 18, 1995; RFC 930, Modifications to ICD Table 1, Appendix A Tables 11 and 12, Appendix B data flow diagram and notes, and Appendix D data flow diagrams and notes; RFC 931, the IN/FBI FCE Physical Layer Interface, the CJIS WAN will not be the local demar side of the CSU/DSUs as specified in Article 4.1.1.1., Physical layer Interface of the IAFIS ICD; RFC 932, remove references to ITN controlling security for IAFIS from the ICD; RFC 935, modify IAFIS messages A1003, A3026, and E1003 in the MDD to include additional fields to support transmit of electronic rap sheet; RFC 938, Modify Table 3-1 in ICD to include photo delete, and photo retrieve request; RFC 939, adds requirements to support IAFIS Filtering. The changes provide the functions necessary to control the release of data on special subjects contained in the IAFIS data files; RFC 870R2, need to develop a concept of operations for Latent Search. Need to define/verify the requirement for the service provider to cancel searches; RFC 944, defines three non-operational environments—training, test and development; RFC 946 modify MDD sets to include "IDC" field; RFC 947, the ICD—specified Nlets to IAFIS interface protocols do not reflect the current Nlets Configuration, a modification to the ICD is needed to describe the current interface; RFC 949R3, added requirement to notify originator of Wants and Flashes when IAFIS detects criminal activity; added requirement to process Wants and Flash Update Notification message ($.A.WPT) received from NCIC 2000; RFC 955R1, to better explain the IAFIS Special Latent Cognizant functionality and to resolve inconsistencies; RFC 956, modifies requirements for blocking messages based on information contained in the Multiblock Header Code; RFC 972, add message A1802 to Tables 3-1 and Table 11.0, changed messages A1022 and A1027 to meet Build C Requirements, modify the IAFIS Header (IAFISHDR); and RFC 993 which incorporates changes from ECP003 negotiations and administrative changes.

I. IAFIS-IC-0020(V8), June 6, 1997—This version release is a single-sided document and will be managed as such hereafter; additionally, this version includes changes to the "Standards and Guidelines" to reflect IAFIS CCB direction to have common baselines across segments, updates/changes were made to: the IAFIS Systems Requirements Definition (SRD); the IAFIS System Specification; the IAFIS Interface Control Document (ICD); and the CJIS Electronic Fingerprint Transmission Specification (EBTS). This document incorporates the following RFCs: 953R1; 961; 971R1; 973;

974; 975; 976; 977; 978; 979; 980; 981; 982; 983; 984; 985; 986; 987; 988; 989; 990; 998R1; 1002; 1003; 1004; 1005; 1006R1; 1008; 1009; 1010; 1012; 1015; 1021; 1022; 1023; 1047R2; 1048R1; 1025R2; 1026; 1027; 1033; 1045; 1046; and 1076.

J. IAFIS-IC-0020 (WD)—Working Draft, November 7, 1997—This version release is a Working Draft provided to facilitate the RFC writing process. This working draft incorporates the following RFCs subject to the aforementioned limitations: 1035R3, 1040R1, 1043R1, 1044R1, 1050R1, 1051R3, 1053R2, 1055, 1056R1, 1057R1, 1058R1, 1060R1, 1062, 1064R1, 1065R1, 1066R3, 1067R1, 1069R1, 1070R1, 1071R1, 1072R2, 1073R1, 1074R1, 1075R1, 1078R1, 1079R1, 1080R1, 1082R1, 1084R1, 1085R1, 1086R2, 1088R1, 1090R1, 1093R1, 1095R1, 1096R1, 1097R1, 1098R1, 1099R1, 1100, 1102R1, 1104R1, 1109, 1113R1, 1115R1, 1118R1, 1120R1, 1121R2, 1122R2, 1126, 1127R1, 1128R1, and 1139.

K. IAFIS-IC-0020 (V9), March 31, 1998 —This version release incorporates the following RFCs:

1035R3—Modifications to MDD Messages: E1013-Electronic Latent Submission Response, A1016-Latent Feature Search Candidate List, A1020-Ten-Print Fingerprint Search, E1020 EFTS Ten-Print Fingerprint Search, A1021 Latent Search, E1021 Electronic Latent Search, A1028 Latent Features Search, A1034 Latent Search Candidate List. Modified the following MDD Sets: T2LATENT, T2LSR, T2SRL, T2TP, T7USRIMG, and T9TRANS. Creation of new MDD set: ILFSD. Deletion of MDD set: T2TPFS. Creation of new MDD elements: AFV, FGP-N, IDC-B, LEN-B, ULF. Modifications to: CIN, CIX, CRP, DLT, EAD, FNR, LCX, MIN1, MRC, MATCH-SCORE, OCA, OFR, RDG, SEX, SOC, CAN, NCR, DOB2.

1040R1—Revise affected documents and applicable message elements to include country of citizenship (CTZ) as a data element in the III/FBI database.

1043R1—Modified element AAC. Created a new MDD message A3314, SEARCH STATUS FOR NON-IDENT, NON-RETAIN, TEN-PRINT SUBMISSIONS. Added "NOTE: A3314 to Figures 21.1-01a steps (11, 12), 21.1-01b steps (11, 12) and 21.1-01c steps (15, 16) Update dataflow charts.

1044R1—Element format types (numeric, alphanumeric, and alphanumeric special) were corrected for elements ICN, SCN2, SERV, MTY, and ERRC in ICD Appendix A, Message Definition Database (MDD).

1050R1—Modified existing elements to be consistent with ICWG agreements: env-removed unnecessary restrictions, gca-added permissible values, hll-added permissible values, icn-no longer allow a blank as a special character, ipri-added permissible values, isize-added permissible values, need-added permissible values, rsnd-corrected the permissible values, vll-added permissible values, mfn-changed length, added example.

1051R3—Change made to Data Flow Diagram Figure 21.1-01a Sequencing and Notes. Add requirements to Table 4-1.

1053R2—Add requirement for ITN/FBI to validate ORI and Line Number of incoming submissions/requests using ORI File, NCIC Line Number Table, and Type of Transaction. Add requirement for III/FBI to validate ORI using ORI Table, Type of Transaction, and Purpose Code. Add requirement for ITN FE to receive $.A.ORI and $.A.LIN messages from NCIC 2000.

1055—Delete references to Unsolicited Messages A3104, N3104 in DFD 21.1-1 and

21.1-2. Delete A3104 and N3104 Messages from MDD. Delete references to messages in ICD tables 3-1, 12.0 and 14.0. Delete Unsolicited_CNR_Report set in MDD.
1056R1—Adding unsolicited messages A3121, N3121, A3112 and N3112 TO DFD 21.4-7 and 22.3-3 in ICD. Changed message name on N3121, A3121.
1057R1—Deleted flow representing Unsolicited Message on Figure 21.3-6. Changed name of message A1032 from FNU Search to Service Provider Subject Search Request on Figure 21.3-6. Changed name of message A1033 from FNU Search Response to Service Provider Subject Search Candidate Record on Figure 21.3-6. Added flow of message A1029 between III/FBI and ITN/FBI on Figure 21.3-6. Renumbered flows on Figure 21.3-6. Embellished Sequencing and Notes for Figure 21.3-6. Added DFD 21.3-6 to description of message A1029. Modified description of message A3036.
1058R1—Changes to MDD elements include: DAT3-Added restrictions, DATE-TIME-Added restrictions, IMAGEC-Changed maximum size to 70,000, IMP-Added description, example, and restrictions, ISR1 Fixed description and format added restrictions. TMR-Added restrictions. Changes to MDD Set: ASRR-Changed maximum number of occurrences to 20.
1060R1—these changes allow the current Queued Response and No Response message protocols to include an optional transfer of message data in a file named within the requesting message. This file transfer option is then applied as noted herein to all ITN-AFIS messages, which may include images.
1062—Delete MDD messages A3080, A3081, and A3082. Change Data Flows 21.3-17 and 21.3-18 and replace the deleted messages with already existing messages A1040 and A1042. Add CONDITION information to messages A1040 and A1042. Correct ICD tables 3-1, 12.0 and 14.0, removing the three messages.
1064R1—Deleted flow representing Unsolicited Message on Figure 21.3-12. Changed name of message A1032 from FNU Search to Service Provider Subject Search Request on Figure 21.3-12. Changed name of message A1033 from FNU Search Response to Service Provider Subject Search Candidate REC on Figure 21.3-12. Added flow of message A1029 between III/FBI and ITN/FBI on Figure 21.3-12, Renumbered flows on Figure 21.3-12. Embellished Sequencing and Notes on Figure 21.3-12. Embellished message A1029 definition (added dfd 21.3-12). Corrected and embellished message A3040 definition.
1065R1—Deleted figure 21.3-11—External Record Sealing Request Data Flow. Incorporated A3124 message into Unsolicited Message flow and deleted from Figures 22.3-1, 22.3-2, and 22.3-3. Add flow for A3045 message to Figure 22-3-1 and 22.3-2 for file synchronization. Add flow for A3150 message to Figures 22.3-1, 22.3-2, and 22.3-3 for unsolicited reports. Added flows for A3312 and A3311 to figure 22.3-1 and 22.3-2 for file synchronization with AFIS. Updated sequencing and notes for Figure 22.3-1, 22.3-2, and 22.3-3. Added reference to Figure 22.3-1, 22.3-2, and 22.3-3 to definition of message A3150. Added reference to Figure 22.3-1 and 22.3-2 to definition of messages A3045, A3311, and A3312. Updated definitions of messages A3207, N3207, A3208, N3208, A3209, N3209, A3210, N3210, A3211, N3211 A3212, and N3212.
1066R3—Modified Figure 21.3-8 Sequencing and Notes. Modified message definitions A1029, A3027, A3029, A3031, A3045, A3150, A3311, A3312, and A3321.

1067R1—Deleted flow message A3031 from III/FBI to ITN/FBI in Figure 21.3-7. Deleted flow message from A3027 from ITN/FBI to III/FBI in Figure 21.3-7. Added flow for message A3045 from III/FBI to ITN/FBI in Figure 21.3-7. Deleted flows for messages A3124 and N3124 and incorporated into the notes for the Unsolicited Message flow in Figure 21.3-7. In Figure 21.3-7 deleted flow for messages A3031 from III/FBI to AFIS/FBI and A3027 from AFIS/FBI to III/FBI. Added flows for messages A3321 and A3312 from ITN/FBI to AFIS/FBI, and A3311 from AFIS/FBI to ITN/FB in Figure 21.3-7. Added flow from III/FBI to ITN/FBI representing desk-top printer reports in Figure 21.3-7. Renumbered flows and embellished sequencing and notes for figure 21.3-7. Added information to descriptions of messages A3205 and A3206. Added Figure 21.3-7 to DFD list for message 3045. Changed mate of message A3312 to A3311 instead of A3027.
1069R1—Changed Messages A1090, A1091, A1092, A1093 and E1000. Changed Message Sets T2CPD, T2CPR, T2PDR and T2PRR. Replaced Set T10TRANS. Changed MDD elements CGA, CSP, DAT, HPS, HLL, PHD, POA, POS, RES, SLC, SRC, and VPS. Added MDD elements IDC10, IMT10, PXS10 and VLL10.
1070R1—This RFC created MDD messages: A1007 Unsolved Latent Match (Internal); A1017 LPS ULF Latent Search; A1019 LPS ULF Search Response; A3302 Unsolved Latent Image Add Response; A3322 Internal Unsolved Latent Delete Request and A3354 Internal Unsolved Latent Add Confirm. Modified messages: A1004 Response Data—Unsolved Latent Match; A1005 Unsolved Latent Match (External); E1005 External Unsolved Latent Match; A1018 LPS ULF Ten-Print Search; A1055 Unsolved Latent Fingerprint Image Request; A1056 Unsolved Latent Fingerprint Image Response; A3301 Unsolved Latent Image Add; E3325 External Unsolved Latent Delete; A3325 Delete Unsolved Latent Record Request (Ext.); A3326 Unsolved Latent Image Delete; A3327 Unsolved Latent Image Delete Response; A3328 Delete Unsolved Latent Record Response; A3329, Unsolved Latent Delete Response (External); E3329, External Unsolved Latent Delete Response; A3341 Unsolicited Unsolved Latent Delete; A3342 Unsolicited Unsolved Latent Delete (External); E3342 External Unsolicited Unsolved Latent Delete; E3351 External Unsolved Latent Add Confirm; A3351 Unsolved Latent Add Confirm (External); A3352 Unsolved Latent Add Confirm Response; A3353 Unsolved Latent Add Confirm Response (External); and E3353 External Unsolved Latent Add Confirm Response. New MDD Element/Set: T2ULAC, T2ULAR, T2ULD, T2ULDR, T2UULD, T2ULM, MSG-Reason/Status/Error/Message, and ASCN-AFIS Segment Control Number (EFTS). Modifications to Existing Data Flow Diagrams: 21.1-01 External Ten-Print Submission Data Flow, 21.1-02 Internal Ten-Print Submission Data Flow, 21.5-01 Remote Latent Search Data Flow, 21.5-02 External Latent Submission Data Flow, 21.5-03 Internal Latent Submission Data Flow, 21.5-04 Internal Unsolved Latent Search, 21.5-05 Internal Unsolved Latent Delete Data Flow, 21.5-06 External Unsolved Latent Delete Data Flow, 21.5-07 Internal Unsolved Latent Add Confirm Data Flow, 21.5-08 External Unsolved Latent Add Confirm Data Flow, and 21.5-09 Unsolicited Unsolved Latent Delete Data Flow—DELETED.
1071R1—Delete messages to/from IDAS A1025 ATS Request, A1026 ATS Response, and A1130 IDAS File Maintenance Request. Delete message to/from ITN/IAFIS FE, A1050 Fingerprint Image Request, and A1060 Fingerprint Image

Submission. Delete request/response messages for fingerprint extraction data, A1100 Request Fingerprint Feature Extraction, and A1101 Fingerprint Feature Extraction Response. Deleted unnecessary messages A1808 NCIC 2000 Wanted Persons Inquiry, A1809 Person Hit Response, and A3300 Latent File Maintenance Request. Delete unused sets AST-1 ATS Search Request, AST-2 Subject Search Request Response, and IDAS-FM IDAS File Maintenance.
1072R2—Changed ICD Tables 3-1, 11.0, 12.0, and 14.0 to add A3403/N3403 and delete Messages A1808/N1808, A1809/N1809, A1811/N1811, and A1812. Message A1812 is replaced by message A3150. Changed Figures, Sequencing, and Notes to revise Want and Flash processing in data flows 21.1-1, 21.1-2, 21.1-4, 21.3-2, 21.3-3, 21.3-4, 21.3-6, 21.3-8, 21.3-10, 21.3-12, 21.3-13, 21.3-16, 21.3-21, and 21.4-2 to reflect Want and Flash processing. Change ICD Sequencing and Notes to delete A1811/N1811 and Want and Flash processing from data flows 21.2-1, 21.2-3, 21.3-10, 21.3-11, 21.3-14, 21.3-15, 21.4-3, 21.4-4, 21.4-5, 21.4-6, 21.4-7, 21.5-2, 21.5-3, 21.3-1, 22.3-2, and 22.3-3. Revise MDD messages A1312 and A1313 to reflect Want and flash processing. Revise MDD report "III IDENT MESSAGE—ONLINE HIT NOTIFICATION" used in A3403/N3403 to include III DEC with FII.
1073R1—This RFC corrects the ICD Data Flows identified: 21.3-16 External Criminal Print Ident Data Flow, 21.4-01 External Criminal History Request Data Flow, 21.4-03 External Subject Search Data Flow, 21.4-05 External III/FBI Administrative Inquiry (ZI) Data Flow, 21.4-06 External III/FBI Availability Inquiry (ZR) Data Flow, and 21.4-07 External III/FBI Record Status Inquiry (ZRS) Data Flow.
1074R1—Includes the following messages and set changes: MDD Message A1023-Conditions: delete condition. MDD, Set T2ERRI: Changed/corrected Set Format and Contents. FNU mandatory; SID optional. MDD, Set T2ERRL: Change CIN to 1 to 5 occurrences; change CIX to 0 to 5 occurrences.
1075R1—Administrative corrections to the following: RFC 1006R1-Changed HGT1 to HGT in set "LDSSR." Corrects error; HFT already is listed in contents of set. RFC1021-Set T2NAR: delete second occurrence of o("2.060" + MSG+"GS")38. Corrected format/Syntax of Set. Corrected FFN from optional to mandatory. Format errors in T2NAR have also been corrected.
1078R1—MDD messages created: A3067 Latent Penetration Query Response Data, A3068 Latent Repository Statistics Response Data, A3069 Latent Search Status and Modification Response Data, A3070 Internal Latent Search Penetration Query, A3071 Internal Latent Search Penetration Response, A3072 Internal Latent Search Status and Modification Query, and A3073 Internal Latent Search Status and Modification Query Response. MD messages modified: A3061 Latent Search Penetration Query, A3062 Latent Penetration Query Response, A3063 Latent Repository Statistics Query, A3064 Latent Repository Statistics Response, A3065 Latent Search Status and Modification Query, and A3066 Latent Search Status and Modification Response. Modifications to existing set descriptions: T2LPNQ Latent Penetration Query, T2LPNR Latent Penetration Query Response, T2LRSQ Latent Repository Statistics Query, T2LRSR Latent Repository Statistics Response, T2LSMQ Latent Status and Modification Query, and T2LSMR Latent Status and Modification Response. Modifications to existing element descriptions: CFS-Cancel Fingerprint Search, PEN-Penetration Query Response, and RSR-Repository Statistics Response.

Modifications to existing Data Flow Diagrams: 21.5-10 Internal Latent Search Penetration Query Data Flow, 21.5-11 External Latent Search Penetration Query Data Flow, 21.5-12 Internal Latent Repository Statistics Query Data Flow (DELETED), 21.5-13 External Latent Repository Statistics Query Data Flow, 21.5-14 Internal Latent Search Status and Modification Query Data Flow, and 21.5-15 External Latent Search Status and Modification Query Data Flow.

1079R1—Updated ICD tables 3.0, 3-1, 11.0 and 14.0. Add new Data Flow number 21.1-4 with Sequencing and Notes. Add new messages A1043 and A1044. Delete set structure CIVIL-IDENTIFICATION-DATA. Delete element HGT2 and HGT1.

1080R1—Revised SET structure "T9TRANS" to reflect the EFTS type 9 records to include minor changes.

1082R1—Replaced Figure 21.3-14. Restore FNU Request Data Flow with data flow of same number and title. The new workflow has the following messages: A1008 Restore FNU Query from ITN/FBI to III/FBI; A1009 Restore FNU Query Response from III/FBI to ITN/FBI; A1033 Service Provider Subject Search Candidate Record from III/FBI to ITN/FBI; A3407 Restore Criminal History Request from ITN/FBI to III/FBI; A3027 File Maintenance Response from III/FBI to ITN/FBI; A3045 File Synchronization Request from III/FBI to ITN/FBI; A3310 Update Fingerprint Features Request from ITN/FBI to AFIS/FBI; A3311 Update Fingerprint Features Response from AFIS/FBI to ITN/FBI; A3331 File Maintenance Completion Notification from ITN/FBI to III/FBI; A3150 Unsolicited Report from III/FBI to ITN/FBI; and A1011 Cancel FNU Restorability from III/FBI to ITN/FBI. Deleted message A3409, Restore Features Request. Added 21.3-14 workflow to message definitions A3027, A3310, A3311, A3331, A3117, and N3117. Created new messages A1008, A1009, and A1011. Modified A3407; added 21.3-14 workflow. Modified A3045; added 21.3-14 workflow. Modified A1033; added 21.3-14 workflow. Modified A3150; added 21.3-14 workflow. Modified FST element, AAC element, MSGCOD table. Removed TBDs of RST element and specified codes for Consolidation, Subject Expungement, and Deceased. Modified RPTDEST to include destination for post-consolidation information. Modified Tables 3-1, 11, 12, and 14 to accommodate above. Modified Segment Specifications to incorporate the changes necessary to accomplish the actions required for Restore FNU.

1084R1—This modification added Appendix C containing IAFIS error message definitions to the ICD.

1085R1—Updated Data Flow Diagram 21.3-21 sequencing and notes; delete the old DFD 21.3-21 and replace with the new DFD 21.3-2; modify messages A1032, A1033, A1048, A3027, A3045, A3105, A3311, A3312, A3404, L1048, L3404 and N3105; change the PARTIAL-EXPUNGEMENT-DATA set; add a new element TOS_NUM; and add new code table TOS_NUM.

1086R1—Add T1$ Test Request. Add DFD 23.4-2. Add new messages A5100, N5100, A5101, and N5101. Add new ACCEPT TI$ Report. Update ICD Tables 3.1, 12.0 and 14.0. Change MDD Element PUR.

1088R1—Add new message N1306. Add messages A1306 and N1306 to DFD 21.4-1. Remove messages A3124 from DFD 21.4-1 and add these messages to Sequencing and Notes. Rewrite Sequencing and Notes on DFD 21.4-1. Update ICD Tables 3.0, 11.0 and 14.0.

1090R1—Delete old Figure 21.3-13 Sequencing and Notes, and Replace with new Figure 21.3-13 Sequencing and Notes. Delete old Figure 21.3-13 DFD and replace with new Figure 21.3-13. Delete figure 21.3-22 in DFD and Sequencing and Notes. Add message A3038. Delete message A3031. In message A3038 add conditions, correct the contents, add a name for ID REC-LEVEL, change TYPE to TPE, change ACH1 to ACH, change Min of OLD-VAL from 30 to 1, and change Min of NEW-VAL from 30 to 1. Changes to SCH Codes include add AON. Correct description of AKA, ANF, AOL, DPE, PHT, ROR, and SOC to match that in the MDD. Change code value from FPC-SET to FPC and from PRO to PRO1 to match what's stored in MDD. Delete messages A3404, L1048, L3404, N3105 in DFD 21.3-13. Delete CIV-IL-MOD-DATA. Added two code values to the Codes table the FST element. Delete element TOD. Added SCHM to the STOT Code Table and deleted subheadings. Modified following messages to reflect changes: N3105, L3404, L1048, A3404, A3321, A3312, A3311, A3310, A3105, A3045, A1048, A3027.
1093R1—The sequence of message flows on this diagram are being reordered. The name of Message A1058 is being corrected.
1095R1—Adds the NARA data flow to the ICD Figure 22.3-6.
1096R1—Added new tables: 14.2-Set Change History and 14.3-Element Change History. Deleted Section 11.0, replaced with Table 11.1 "EFTS Messages," Deleted 12.0, replaced with Table 12.1 "NCIC Messages," Deleted 13.0, replaced with Table 13.1 "Nlets Messages," Deleted 14.0, replaced with Table 14.1 "Unix File" and Section 15.0 "Message Change History" renumbered as Table 15.1. Tables 10.2, 10.3 and 10.4 Deleted. Replaced Table 10.1 with new table. Table 3-1 deleted, replaced with new table. Modified Section 10.
1097R1—Additions of new MDD Messages include: N3601-NCIC Administrative Message, L3601-Nlets Administrative Message. Addition of new Data Flow Diagram: include 22.3-6 NCIC and Nlets Administrative Messages.
1098R1—To provide a File Comparison function which uses bitmaps to provide fast comparisons of the criminal and civil ten-print files. A file comparison function for the Ten-Print Certification File (TPCF) is not provided in this RFC because the TPCF is not suitable for a bitmap implementation. Adds new Appendices E & F, and replaced Figure 22.3-05 Sequencing and Notes.
1099R1—Clarified External Image Request process. Updated other messages returning images to maintain consistency. Adds support to send a summary of the image request responses and note any omitted images to the external user. Made changes to Figure 21.2-3 Sequencing and Notes and DFD. Update reflected in messages: E1050, A1310, A1311, A1051, A1052, E1052, A1063, A1064, E1064, A1054, A1058, A3330 and in Set Levels and Element Levels AMP, T2ISR, T2IRR, T4HIGRAY—RESP, T2IRQ, T2MIR, FNR, SPF-FLAG.
1100—Added image, administrative, and latent error message sets (T2ERRA, T2ERRI, T2ERRL) to the message E1803, External Test Message. Deleted A1803 since message only goes to ITN from the CJIS WAN.
1102R1—The format for the IAFIS Control Number (ICN) was defined and added to the MDD and III/FBI Segment Specification.
1103R1—Created ICD Figure 21.4-08-Ad Hoc Subject Search Data Flow. Created Messages A1132-Ad Hoc Subject Search Request—String, A1133-Ad Hoc Subject

Search Response, A1134-Ad Hoc Subject Search Request—Structure, I3022-Ad Hoc Subject Search Response File Format. Created Elements: AHSPARMS, DOFILE, NUMCANS, MAXCANS, AHSFLD with code Table. Modified Element FVL.
1104R1—Adds requirements to ITN/FBI and III/FBI to enable a special stop service provider to create a criminal record including complete criminal history data and complete fingerprint data. Addition shown in Figure 21.1-02 Sequencing and Notes and DFD.
1109—Correction to Data Flow Diagram 21.3-21 by replacing message A3027 coming from AFIS/FBI to ITN/FBI, with message A3311.
1113R1—Update message A3028, Consolidation File Maintenance Request.
1115R1—Modified the following existing MDD messages: A1065-Record Add, A1066-Record Maintenance Response, A1067-Record Delete, A1069-Copy, A1070-Copy and Delete Maintenance Response. Deleted Existing MDD Message: A1068-File Maintenance Response. Modified Existing Data Flow Diagrams: 21.5-16-Record Add or Update Data Flow, 21.5-18-Delete and Copy Data Flow. New MDD Elements: COPY-ALL-SLC. Deleted Existing Data Flow Diagram 21.5-17 Copy Data Flow. Changes reflected in Tables 11.0 and 14.0.
1117R1—This RFC alters the description of the contents of ICN to allow assignment of ICNs by the AFIS segment.
1118R1—Revise messages A1035/N1035 and A1039/N1039 to be consistent with NCIC 2000 documentation. Correct the format of WCMU1, HDR and NCIC HDR data sets in IAFIS to be the same as these data sets in NCIC, and DFD 21.4-03 to show the correct message response.
1119R1—Appendix D of the IAFIS Interface Document (ICD) is being updated to include report formats that are documented in the III/FBI Response Generation and Supervisor Computer software Configuration Items (CSCIs). Pertinent report formats from other sources have also been included as well. All report formats have been revised to reflect year 2000 date format changes, replacement of IDAS Process Control Number (PCN) identification with IAFIS Control Number (ICN) identifications and minor report format changes.
1120R1—Creates an image buffer for use when transmitting compressed images within IAFIS.
1121R2—Removing of "MIDS" system as a separate segment of IAFIS, to include removal of interface and transmitting of data from other segment to MIDS. Reserved sections 3.6, 4.9 and Section 13. Section 23.1 describes the process of transferring data from III/FBI and AFIS/FBI to ITN/FBI to support Management Information Reporting and User Fee Billing within the segment.
1122R2—Modifications to the ICD/MDD include the addition of new messages (E1011 and E1001),unique to the CSS to enable segregation of CSS input from other input and addition of new MDD sets (T2CARC, T2CNAC, T2DEKC, T2FNCC, T2FUFC, T2MAPC, T2NFFC, T2FNCM, T2FUFM, T2MAPM, T2NFFM, T2NFDP, T2SLCC, T2RSBC, T2CSS-DISP, T7CSS), to support the new types of transactions. These changes required modification to some existing sets and all associated dataflow diagrams. In addition, the ICD was modified to eliminate references to FICS. Associated modifications to the associated ISDD process flow diagrams and descriptive text are included for completeness and reference and help in understanding the

change.
1123—Deleted the Report titled "Multiple FNUs for the One III-State-Pointer" from the following messages: A1036, A1046, A3051, A3053, A3055,
1124R1—This RFC clarifies the description and definition of the MDD T1TRANS set to capture data field differences dependent upon message direction.
1125R1—Replaced the element DAI in the A3026 message with the element CRI.
1126—Delete MDD elements that will not be used by IAFIS. To develop an MDD without extraneous elements.
1127R1—To provide guidance to the three IAFIS contractors during the programming of Build E messages, sets and elements through modification of ICD/MDD messages, sets and elements to meet requirements of the ITWG.
1128R1—Delete MDD Code Tables that will not be used by IAFIS. Modify the contents of the MDD Code Tables that will be used by IAFIS.
1129R1—Modification to ICD/MDD elements, messages, and sets to incorporate the EFTS changes implemented by RFC 1024R2 and RFC 1035R3. Addition of A3107/N3107 to Figures 21.1-01a, 21.1-01c and 21.1-02 Sequencing and Notes.
1130R1—Modifications and deletions to ICD/MDD elements, messages and sets, in Figure 21.5-02 Sequencing and Notes and 21.5-02, 21.5-03 DFD.
1135R1—FICS message F1010 is being removed from the MDD. A1001 message template added.
1136R1—This change returns design of SCH-MOD-DATA to SAIC's design. In the process many changes were added to make message implementation clearer and simpler; e.g., "MANY" used in the ICD MDD as a limit to the possible iterations of a field is difficult to deal with in implementation, so a finite number was decided.
1138R2—The revised IAFIS Error Code Table is to be added to the MDD. This replaces the Error Codes formerly contained in ICD Appendix C. The text of ICD Sections 5.10.3 and 5.10.4 are amended to reference this table in Appendix A, Message Definition Database
1139—Moves portions of the ICD to Appendices to simplify maintenance. Appendices re-organized as follows: Appendix G-IAFIS Data Flow Summary; Appendix H-IAFIS Intersegment Messages; Appendix I-EFTS Messages; Appendix J-NCIC Messages; Appendix K-Nlets Messages; Appendix L-Unix File Messages; Appendix M-Message Change History; Appendix N-Set Change History, and Appendix O-Element Change History.
1141R1—From Figure 21.3-7: Removed Hardcopy Response and Messages L1048, A1048, A3105, N3105, L3404 and A3404. Modified Figure 21.3-7 Sequencing and Notes to reflect deletion of messages and Hardcopy Response. Removed reference to Figure 21.3-7 from messages L1048, A1048, A3105, N3105, L3404 and A3404.
1142R1—This RFC restores the flow of message A1016 from AFIS/FBI to ITN/FBI in ICD data flow 21.5-2. It also adds a flow of messages A1310 and A1311 for the purpose of filtering the candidate list. The following changes are included: Modifies ICD data flows 21.5-2, deletes definition of message A1016. Modifies message A1028, A1310 and A1311. Deletes AFIS requirements to send the candidate list to III/FBI. Deletes associated test table entry. Deletes AFIS requirements 712 and aa05.
1144R1—CONSOL-DATA and messages A1009, A1033, A3331, A3045 modified. A1011, Cancel FNU Restorability message deleted. Appendices G, H, and M and

DFD 21.3-14 and notes modified to reflect the changes as well as to clarify several notes: (a), (b), and (c).
1147R1—MDD messages have been allocated to Builds E, F.1 and F.2 according to the priorities assigned within RFC 1146, Builds E/F.1/F.2 Requirements Allocation Tables. The build assignments contained within the attachment will be added to the MDD for each message by Data Flow Diagram. The table is current with the engineering version of the MDD, V9DF. RFCs 1141, 1142 and 1144 have additionally been incorporated. Changes associated with these three RFCs are noted in the RFC/ACSN column within the table.
1149R1—The MDD Validation effort reconciled changes to the MDD resulting from previously approved RFC. During the validation process, additional errors were discovered that were not addressed by previous RFC.
1150R1— Modified message A3150 in the following Data Flow Diagrams: 21.01a, 21.01b, 21.01c, 21.1-02, 21.3-02, 21.3-04, 21.3-06, 21.3-08, 21.3-12, and 21.3-21
1153R1-Change the Maximum size of latent search candidate lists from 999 to 99 in messages A1016 and A1034.
1154R1—This RFC creates a new message Special Stops File Maintenance Request A3041, set SPECIAL-STOP-DATA, element TYS, STOT SSM (Special Stops Modification), and error code L0017. The Special Stops Modification Functionality is added to DFD Internal SCH (CCNR) Modification Request and updates the corresponding sequencing and notes. In addition it corrects the name if set SUBJ-SRCH-DATA and fills in the permissible values for the element AUD.
1156R1—This RFC resolved issues presented by SAIC as a result of preparing their ECP005.
1158R1—Change message A1019 (LPS ULF Search Response) to return up to 99 candidates instead of just 1. The Add ULF Image (A3301) and Delete ULF Image (A3326) should be made NR protocol instead of KR protocol and delete the response messages A3302 and A3327.
1159R1—Change SLC search message so that both the A1027 (TP Search Request) and the A1028 (Latent Search Request) will search only 1 SLC repository. Reinserts into Table 8, requirements 3.2.1.2.7[679] and [706].
1160R1— Added detail to the definitions of each of the elements used in set IAFISHDR, including: AUTH, DATETIME, DAT3, ERRC, E NV, ICN, IPRI, MTY, MVN, NEED, ORI, OSG, RSND, SCN2, SERV, STOT, TMR, TSG. Adds and updates code table for AUTH and SERV.
1161R1—Added the following codes to the DESTPRT code table: 06-Reserved (change code 02 to:'NCIC Reject Printer'; 07-III Staff Printer; 08-Service Desk Printer; 09-Software Support Group (SSG).
1162R1—Modified DFDs 21.1-01a, 21.1-01b, 21.1-01c, 21.1-02, 21.1-07(new diagram) and 21.2-01.
1165R1—Provided updates to the following: MESSAGE LEVEL A3016, A3340, A3301, and I3020. SET LEVEL CIVILFM, T2SRE, T7CSS, T2CSS, and IMA is new. ELEMENT LEVEL MAK, MODL and SERNO are new. Deleted DAT2. Modified EID, PUR, SID and MNU. Modified Code Tables SGT, and AKA.
1167R2—Modified the contents of Message A3010-Ad Hoc CCA Search Request.
1169R1—Modified sections 5.10.1, 5.10.2, 5.10.3, and 5.10.4. Update Table 5-1. In-

tersegment Message Error Types. Figure 21.6-01 added Transaction Error Data Flow. A1801 EFTS Error Response Request—Replaces individual elements with ERRMSGDET set. Corrected use of CIN data. Add MSG elements for service provider rejection text. The new STOT of ERRA is added to the STOT Table. A1802 Error Notification—Correct description of protocols used by message and mates of message. ERRMSGDET set-Allows use of MSGCOD values which need no additional descriptive parameters. T2ERRA, T2ERRI, T2ERRL, AND T2ERRT sets corrects change made RFC 1130 so that up to 11 error descriptions may be reported in response to one EFTS submission. Error CODES Table Expands list of error and clarifies meaning of errors.
1170R1—Updated the TOT, STOT and MKE/MTC Code Tables.
1171R1—Corrected A3311 to allow no PTRC values returned after an AFIS/FBI FNU delete.
1172R1—Modified Process Control Code (PCC) in code table.
1173R1—CIVILDESCRIPTIVEDATA Set is being removed from A3310 and A3025. DESCRIPITIVEDATASET is being modified.
1174R1—Section 2 Applicable Documents added (m. IAFIS Filtering Rules 12/97). Section 3.3 New Section titled Special Stop Filtering. Modifications in DFD Sequencing and Notes: 21.1-01a, 21.1-01b, 21.1-01c, 21.1-01d, 21.1-02, 21.1-05, 21.1-06, 21.1-08, 21.2-03, 21.2-04, 21.3-02, 21.3-03, 21.3-04, 21.3-06, 21.3-07, 21.3-08, 21.3-10, 21.3-12, 21.3-13, 21.3-14, 21.3-16, 21.3-17, 21.3-18, 21.3-21, 21.4-01, 21.4-02, 21.4-04, 21.5-01, 21.5-02, 21.5-03, 22.3-01, 22.3-02, 22.3-03.
1175R2—Modified Want/Flash Requirements Data Flow Diagrams Sequencing and Notes in Figures 21.1-01a, 21.1-01b, 21.1-01c, 21.1-02, 21.1-05, 21.1-06, 21.3-02, 21.3-03, 21.3-04, 21.3-06, 21.3-07, 21.3-08, 21.3-10, 21.3-13, 21.3-16 and 21.3-21. Delete messages A1314, A1315. Consolidate A1314 with A1312 and A1315 with A1313. Delete all T1 and T2 data from A1312 and A1313. A1810/N1810 Change the name to NCIC Want Notification. Add message A1811 as Want Notification. Delete messages A1813/N1813, A3403/N3403. A3401/N3401 Add two reports. Corrected contents: FLASH-NOTICE-DATA, EW, MW, LW, CW, and XW sets. Add example DCL, DOR3, EXT, FLC and RCA. Correct typo-DOC, Correct Permissible Values-DOW, Correct one code-RFR codes, Correct format RRE, STOT and TOT Codes: Add CQ, EW, MW, LW, and XW; and delete $.A.WPT. Delete TOF Codes. Delete element WRR. Delete ICN from the set-Want-Notice-Data.
1177R1—This RFC constitutes a complete revision of Sequencing and Notes that accompany the Data flow Diagrams in the Interface Control Document.
1180 —This RFC fixes errors in RFC1162R1 to enable proper implementation of Messages E1005, A1055 and A1056.

L. IAFIS-IC-0020 (V10), April 1, 1999 —This version release incorporates the following RFCs:
1178—The MDD Element of Latent Case Number (LCN) was revised to be an 11 character alphanumeric-special character.
1179R1—Added two columns to the POB Code Table: CTZ and State. Modified the element definitions for CTZ, GEO, SIG and SID.
1181R1—Replaced "Section 6" with "NCIC." Added NCIC administrative messages. Modified III CPI message. Updated table of contents.

1182R1—Deleted QH Response, and four unused sets from MDD: IH-III-USMS-MSG-0, IH-III-USMS-MSG-1, III-PART-FM-REQ and III-PART-QUERY-REQ. Added NCICHDR to message A3124 and update the report in Appendix D.
1183R1—Modified SPF Code Table, and Elements: PHT, EXP, TSSRR,TP-IDENTIFICATION-DATA, and Message A3026. Deleted PHO Element.
1184R1—Modified MESSAGE LEVEL(s): A1310, A1311, A3007, A3025, A3027, A3043, A3340 to recommend messages using the Queued Response (KR) protocol be changed to use the Immediate Response (IR) protocol, and A3328 be changed to add the No Response (NR) protocol. Removed A3331 as a mate to the A3027.
1185—Modified MESSAGE LEVEL(s): A1034, A1053, A1054, A1024 and E1024 to indicate single fingerprint image returned per candidate, up to the NCR in the Remote Latent Search. Modified MESSAGE LEVEL A1034 to make the element NCR mandatory.
1186R1—Made various changes to STOT data in the element level and code table.
1187—Modified MESSAGE LEVEL: A3314 to allow simplified processing for the Build F1/F2 AFIS Ten-Print notification functions from ITN.
1189R1—Created new element (NEW_ORI) and added it to the set CCA-UPDATE-DATA and deleted elements SMTPAD and RNNRM from the contents of the CCA UPDATE-DATA Set. Modified Code Table (CCC CODES).
1190R1—Messages A3312 and A3321 will be changed from a KR response to a NR response to simplify the IAFIS interface.
1191—New Appendix P, titled "Message Validation Materials"
1192R2—Corrections to existing definitions of a number of elements contained in the MDD.
1193R1—Data Flow Diagrams 21.3-17, 21.3-18 and 21.4-02 consolidated into 21.4-02. Build information for messages added to DFDs.
1194R1—Modified Data Flow Diagrams and Sequencing and Notes. Modified **message**: A1005, E1005, A1037, A3069, A3072, A3073, A3203; **set level**: T2CFS and T2SRL; **element level**: IMG and IMAGEC. New element: EFTS_SCO and DESC-DATA-FLAG.
1195R2—Modified SET LEVELs: PAT, RCD1, RCD2, T2LFFS, T2LFIS, T2LPNQ, T2TPFS and T2TPIS
1196R1—The External, Internal and Description fields in "HAI" and "SMT," of the MDD Code Tables have been updated to reflect changes with the IDAS system.
1188R1—Removed A1033 message from the Restore FNU Request DFD 21.3-14. Modified A1009 Restore FNU Query Response.
1197R2—Clarified the descriptions of codes in the TYS Code Table and the description of the SPECIAL-STOP-DATA set. New DFD 21.3-22. Clarified in Sequencing and Notes to which STOTs the DFD applies.
1198R2—Unused date fields have been deleted, restrictions have been reviewed and corrected, and remaining 6-character date fields have been changed to 8-character formats.
1199R2—Modifications for National Sexual Offender Registry (SOR) in Figures: 21.1-01a, 21.1-01b, 21.1-01c, 21.1-02, 21.1-04, 21.1-05, 21.3-02, 21.3-03, 21.3-07, 21.3-08, and 21.3-16. Added Nlets Administrative Message Formats, SOR Hit Notice and SOR Reject Notice. Modified IDRR, QR, Record Set Report, III Participant ZI

Positive Response and III Participant QH/QWI Response. Added SOR functionality.
1200R2—Added elements to the EFTS Type-9 record to define the IAFIS native mode search format for remote ten-print (STOT=TPFS) and remote latent (STOT=LFFS) searches. Make same changes to associated sets (T2TPFS and T2LFFS).
1201R1—Added a Preliminary response to DFD 21.1-01b and 21.1-01c. Added a Preliminary response report format to Appendix D of the ICD.
1202R1—Revised Sequencing and Notes for sections 21.1, 21.3, 21.4 and 21.5. Replaced ICD Table P-3 with existing table.
1203—Changed Element RCA (Recovery Agency Case Number), to OCA (Originating Agency Case Number) in added sets: MF-SOR-DATA, SOR-ENTRY-DATA and SOR-MODIFY-DATA. An element with the same ID (RCA already existed in the MDD as Recovery Agency Case Number). Updated reports in Appendix D of the ICD to use OCA as the data, the term RCA in printed reports will be changed uniformly to "Case #," followed by the OAC of the registry agency.
1204R1—Build F1 replaced Build E in Message Levels "A3102, N3102, A3103, N3103, A3115, N3115, A3120 and N3120.
1205—Deleted duplicate DFD 21.1-04 assigned in both RFC 1199R2 and 1202R1.
1206R3—Revisions made to Sequencing and Notes and DFDs, Sections 21.1, 21.2, 21.3, 21.4, and 21.5 to maintain synchronicity. Added A1032 Processing Matrix to DFD Sequencing and Notes 21.4-04.
1207R1—Changes to text in Sections 2, 4 and 5, the addition of Appendix C, and new Table P-2 (Appendix P). Corrections and refinements to the definition of NCIC 2000, new message N3602 with an accompanying DFD and Sequencing and Notes. Removal of STX, ETX, and EOT from all NCIC messages.
1208R1—Defines new messages A1059, A1060 and A1061. New sets LDCIVSSR and CIVIL-SUBJ-SRCH. Adds new STOT (CRSS). Figure 21.1-01d redlined "NFMA." Added a new Data Flow diagram and Sequencing and Notes 21.1-09 Civil Record Subject Search.
1209—Adds "Record Set Report (Civil)."
1210—Adds the element CAND-LIST-FLAG.
1211R1—Corrects the two US Marshal Message formats.
1212R1—Defines the default value for SOC as empty in TI$ CFN and TI$ CFR message when SOC is not present in TI$ Request.
1214R2—Corrects inaccurate or incomplete report titles attributed to message A3150.
1215—Includes Errata changes for A3010 and A3011 needed to fully incorporate RFC 1206R3 into the MDD.

M. IAFIS-IC-0020 (V11), August 10, 2000 —This version release incorporates the following RFCs:
1217R1—Changes requirements to IAFIS for supporting an electronic response to ident EFTS submissions when the subject's record contains active NFF pointers.
1218R1—Corrections to text and DFD Sequencing and Notes for synchronizing ICD with F.2 design.
1219R1—Adds report format for CIDR in Appendix D.
1221—Clarification of S&N for DFD 21.3-10.
1222—Corrects missing strikeouts of Missing Persons and Amnesia Victims in Se-

quencing and Notes for DFDs 21.1-01a, 21.1-01b, 21.1-01c.
1223—Clarification of Section C.5.1 as a result of implementation of RFC 1218R1.
1225—Incorporates all MDD Errata changes through May 7, 2000, thus making the Errata (CISA 005) Obsolete. It reflects the as-built configuration of IAFIS.

CHANGE HISTORY PAGE

Version /Revision	Revision Date	Description Of Change	QA Approved	Date
V11R1	17-May-2001	NOTE: With this document revision, the CAO/CM/DMG assumes the administration of approved changes. Incorporated SP/CR: 12386 (Session # 38). Remove all Orphan Code Tables, elements, set and subsets from MDD		
V12	27-Jul-2001	Incorporated SP/CRs: 12020c MDD (Session # 25); Documentation for MDD to reflect change that CRI is mandatory in A1030 messages. 12147b MDD (Session # 20); Change the MDD to reflect CRI as optional in the T2IRQ set (used in the E1050 message). 12323b MDD (Session # 28); Add Purpose Code 'X' per National Crime Prevention and Privacy Compact Council for emergency placement of children. 12324b ICD (Session # 36); Modify the Felon Identification in Firearms Sale (FIFS) Program flagging of criminal history records in III..... 12335a ICD; Documentation SP/CR for NCIC line validation change (TABLE). 12385b MDD (Session # 37);Update the MDD to allow a period in the CPL element. 12612 MDD (Session # 40); ULF Element in MDD A1019 Description in incorrect. BY: [redacted]	b6 b7C	

Version /Revision	Revision Date	Description Of Change	QA Approved	Date
V12R1	. 06-Nov-2001	Incorporated SP/CRs: 12482c MDD (Session # 35); Documentation for MDD in support of TPRS. 12482b, 13466a, and 13465c MDD (Session # 16); Update TOT and STOT Code Tables. 13465c MDD (Session # 41); Add Message A3027 File Maintenance Response and update for Single Maser Conversion. BY [redacted]	b6 b7C	
V12R1	06-Nov-2001	Incorporated SP/CRs: 12902, ICD: Provides for clarification of Appendix P, Table P-3 and to add Column I for INS Remote. 13465c, ICD: Added Figure 21.3-23 Master Record Conversion Data Flow Sequencing and Notes. 14105, ICD: Added Appendix Q—Invalid STOTs Found on the Operational Environment. BY: [redacted] NOTE: This document was prematurely rolled to V12R2. To have the ICD and the MDD (Appendix A) agree in date and time, the official version is V12R1. BY: [redacted]	b6 b7C	

Version /Revision	Revision Date	Description Of Change	QA Approved	Date
V13	20-May-2002	Incorporated SP/CRs: 12853d, MDD (Session #39): Change SMT in ITN to add RTAT; to be in sync with the tattoos used in NCIC; and to correct misspellings (MDD); 13228a, MDD (Session #45): MDD changes in support of PI903; 13466c, MDD (Session #46): MDD Modifications/Additions for Case Latent PI 801; 13671c, MDD (Session #49): MDD changes for response generation banner changes; 13087b, MDD (Session #50): USMS-Add documentation for the A3124 and N3124 messages; 13757c, MDD (Session #51): IISS high priority-Special Stops- All document service providers should be restricted from viewing IDRR, NIDR and record sets for records containing SPF 5 or 6 (A1040 message); 13800d, MDD (Session #56): Modify III permissible values of the Court Offense Literal (COL) and Other court Sentence Provision Literal (CPL) elements; 14217c, MDD (Session #60): MDD changes to the Code T T Stops- All document service providers should be restricted from viewing IDRR, NIDR and record sets for records containing SPF 5 or 6 (A1040 message). 14263, MDD (Session #52): MDD Change protocol for A1063 from NR to KR for IRQ transactions; 14287d, MDD (Session #55): Special Stops—Retain in Civil Retention not printing A3150 or suppressing response when ONC is set; 14292, MDD (Session #54): MDD Correction-A3025 message does not contain RET code as reflected in MDD; 13466c, ICD: Added Figure 21.5-19 Unsolicited Post Latent Search Candidate Processing Data Flow Sequencing and Notes 13757c and 13757a, ICD: Changed Figure 21.4-02—Special Stops filtering. 14281d, ICD: ORI Edits for US Navy and Marine Corps (Appendix P-2).		

Version /Revision	Revision Date	Description Of Change	QA Approved	Date
V13R1	02-Aug-2002	Incorporated SP/CR: 15295b, MDD: A1014 message making the FFN from mandatory to optional field		
V13R2	15-Nov-2002	Incorporated the following SP/CRs: **13775b MDD (Session #62)** – ITN Additional AON values – MDD documentation **14507h ICD & MDD (Session #63)** – Remove response monitoring messages L 3403 and A3404 from IAFIS Dataflow Diagrams-they are not being sent **14956e ICD** – Special Stops – MRD Disposition, CPI, FIS and Internal Criminal History Request for OFO User only response changes. (ICD) **15036b ICD** – ORI Edits for ORIs with K in position nine. (ICD) **15083c MDD (Session # 69)** – MDD Update for IISS requested change for NFFC literal **15319 ICD** – Update the sequencing and notes for TPRS **15391c MDD (Session #65)** – Update ITN MNU Code Table to match NCIC (MDD) **15573c MDD (Session #67)** – MDD change to make OCA field compliant with EFTS **15813 MDD (Session #68)** – MDD – Correct typo in Environment element. Note: The following SP/CRs were previously incorporated into the MDD but not reflected in the change history page: **12482b MDD (Session #35)** – MDD changes in support of TPRS **13466d MDD (Session #16)** – UPLP needs to be added to III STOT code table		
---	---	NOTE: This reflects SPCR 14884 — Convert the IAFIS Interface Control Document (ICD) from WordPerfect to Word.		

b6
b7C

Version /Revision	Revision Date	Description Of Change	QA Approved	Date
V13R3	13 – June – 2003	14942c – Special Stops-On III transactions of EHN and XHN, send A3150 (Hit 5/6) Online Printer Response to Special Stops printer in addition to the A/N3124 already generated to USMS.;15088c – SOR-Modify CC edits for RED to match NCIC existing edits. (MDD); 16014i – Delivery of NFF Record Response Enhancement sequencing and notes for ICD.; 16458 – Update Appendix E of the ICD for the rules for FNU generation; and	[redacted]	18 June 03 25 June 03 18 June 03
V13R4	15-September-2003	17064 – ICD Appendix D behind on updates – Update ICD Appendix D to be consistent with III Pspecs, 17370 – MDD and ICD Updates in support of Hot Check, 16236c – Update the ICD/MDD for the changes required by APB IAFIS Enhancement #13, and 17126a – The MDD message format for External Latent LFS E1010 is not in compliance with the EFTS	[redacted] Still Pending [redacted] [redacted]	14 Oct 03 10 Oct 03 10 Oct 03
V14	10-February-2004	13283f – (5.2 Build) ICD MRD DSP and EXP removal of Consolidation Error Condition 17649a – (5.2 Build) ICD MRD Addition of CIDN to MRD DSP/EXP reports 17819w – (5.2 Build) FTTTF – Flight School: ICD with New STOT=NFAP (Non-Federal Advanced Payment) 17247c – (5.2 Build) ICD MRD DSP Accuracy Rate Recalculation	[redacted] [redacted] [redacted]	18 Feb 04 18 Feb 04 18 Feb 04 18 Feb 04
V15R1	8-June-2004	14500j – Build 5.4) Need to update the IAFIS Interface Control Document (ICD) with $.A.LIN information. The Version was changed from 14 to V15R1 because there were no changes to the ICD for version 15.	[redacted]	17 Jun 04
V16	14-June-2005	SPCRs: 17488b, 18463f, 18465d, 18574b, 19533b, 21497 (ICD). MDD SPCRs: 14507g, 17488d, 18463e, 20370e, 21497, 13466e, 17901c, 17948i, 18305d, 19418c, 19597c, 20000b, and 20122a. See SPCRs for information.	[redacted] (ICD)	7/15/2005

b6
b7C

Version /Revision	Revision Date	Description Of Change	QA Approved	Date
V17	14-September-2005	SPCRs: 20250c, 20501q, 14507e, 18404c, 17727t, 19486d, 19608c, 20309c, 21159c (ICD) ; and 20250d, 18884b, 19318b, 19741d, 20877a, 20149b, 20309d, 20634a, 20680b, 20980c, 21659c (MDD). See SPCRs for info.		9/23/2005
V18	9-December-2005	SPCRs: 207130, 21576i, 22172c, 23146a (ICD); 21122c, 21439e, 21564b, 21576f, 22090b, 22580a (MDD).See SPCRs for info.		03 MAR 06
V19	19-June-2006	SPCR 221100c		15 June 06
V20	15-Febuary-2007	SPCR 25967 NGI updates (version did not go though the CM process)	N/A	N/A
V20.1	30-April-2007	SPCR 25967 Incorporating CAO com-ments and iDSM prototype information		14 June 07
V21	26-July-2007	Version changed as a result of MDD SPCRs 24196v, 27343b & 23461m		27 July 07
V22.0	14-Aug-07	Version changed as a result of SP/CR26510b Incorporated SPCR: 27815d		17 Aug 07
V23.0	14-Nov-07	Incorporated SP/CR's 27519b, 27312b, 27133d, 28760, and 27138c as part of the F8.3 baseline		28 Nov 07
V24.0	16-May-08	Incorporated SP/CR's 28778d (parent), 27491c, 27871e, 27063l, 26791c, 27142g, and 23208d. Associated MDD SP/CR's were 26791b, 27142d, 27871o, 27966, 28194c, and 29465.		11 June 08
V25.0	3-September-08	Incorporated SP/CRs 30113d (parent), 29558b, 28875n, and 29418. Associated MDD SP/CRs were 28875o, 28928a, 29001b, 29159a, 29342b, 29558c, 29730b, 29768c, 29798c, 29888b, 29945h, and 30062a.		08 Sep 08

EXECUTIVE SUMMARY

Interface Control Documents (ICDs) establishes and controls the functional, electrical, mechanical, and protocol information between and among the individual development organizations. The ICD is meant to be a living document which will be updated as design decisions are made to provide timely information on all Integrated Automated Fingerprint Identification System (IAFIS) interfaces. This is the key mechanism to mitigating integration risk.

This ICD defines the external and inter-segment IAFIS mission-critical functional message set. This document defines the following Intersegment Transaction Management Protocols: Immediate Response Protocol; Queued Response Protocol; and No Response Protocol. Also defined are Restart Implications as well as Exception, Error Handling and Web Services

Inter-segment IAFIS internal communication is accomplished through the IAFIS Backbone and Identification Tasking and Networking/Federal Bureau of Investigation (ITN/FBI) Communication Element (BCE), and external communication is through the IAFIS/FBI Front End Communication Element (FCE) (Part of the EFCON/FBI segment). The National Crime Information Center (NCIC) provides external connectivity and NCIC functionality.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION & OVERVIEW

Interface Control Document (ICD) establish and control the functional, electrical, mechanical, and protocol information between and among the individual development organizations. The ICD is meant to be a living document which will be updated as design decisions are made to provide timely information on all Integrated Automated Fingerprint Identification System (IAFIS) interfaces. This is the key mechanism to mitigating integration risk.

This ICD defines the external and inter-segment IAFIS mission-critical functional message set. This document defines the following Intersegment Transaction Management Protocols: Immediate Response Protocol; Queued Response Protocol; and No Response Protocol. Also defined are Restart Implications as well as Exception, Error Handling and Web Services.

Inter-segment IAFIS internal communication is accomplished through the IAFIS Backbone and Identification Tasking and Networking/Federal Bureau of Investigation (ITN/FBI) Communication Element (BCE), and external communication is through the IAFIS/FBI Front End Communication Element (FCE) (Part of the EFCON/FBI segment). The National Crime Information Center (NCIC) provides external connectivity and NCIC functionality.

1.1 Scope

This Interface Control Document (ICD) is for the Integrated Automated Fingerprint Identification System (IAFIS) supporting the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and federal, state, and local users.

1.2 System Overview

The IAFIS Program is a key component of Federal Bureau if Investigation (FBI) efforts to modernize the automated systems that provide identification services to its users. The Criminal Justice Information Services (CJIS) Division staff, systems, and operations are located in Clarksburg and Fairmont, West Virginia (WV). The Latent Print Unit (LPU), which is part of the Laboratory Division, is located in Quantico, Virginia (VA), Dover, Delaware (DE), and Aiken, South Carolina (SC). Portions of IAFIS will also support the Administrative Services Division for special inquiry and background investigations; the Records Management Division for Name Checks; and the National Security Division (NSD) for initial clearance/access at the following Washington, D.C. locations: J. Edgar Hoover (JEH) building, Woodies, Gallery Row, and G Street. Locations not in Clarksburg, West Virginia are referred to as "remote sites."

IAFIS objectives are the following.

- Provide accurate and timely identification services to user agencies. The FBI provides vital identification services support to law enforcement agencies and other users nationwide. To accomplish this mission, the FBI's automated systems must supply needed information in a timely manner. With this support, federal, state, and local law enforcement agencies can identify subjects before they must decide about releasing them from custody.
- Support a paperless environment. Transactions received from and sent to other organizations, as well as FBI internal transactions, will be electronic to the maximum extent feasible. Because not all external organizations will be fully automated, IAFIS will continue to process some paper transactions for many years. CJIS will convert incoming fingerprint cards from paper to digital images and then process them electronically.
- Enable the FBI to process a significant growing workload without increasing staff. The pressures on the federal budget dictate the use of high performance automation to cope with increasing workloads.
- Increase the number of crimes solved by providing enhanced identification services. IAFIS's improved ten-print and latent capabilities will help law enforcement agencies in solving more crimes.
- Provide federal and local agencies with optional levels of IAFIS participation. Each level of participation gives users access to a different predefined level of IAFIS technical capability so that each agency can choose the level best suited to its needs. Agencies may continue to mail ten-print cards to the FBI for fingerprint processing. Agencies with access to live-scan equipment, high speed communications networks, and even their own automated fingerprint identification system may take full advantage of electronic data transmission speeds and access additional IAFIS capabilities.
- Increase national security by identifying individuals who should be prevented from traveling to the United States, or from holding various positions of trust in society. This interoperability effort will permit the Department of Homeland Security (DHS), Department of Justice (DOJ), and their users to seamlessly share identification data that is complete, accurate, current, and timely.

IAFIS provides the following five basic services:

- Identification Services
- Investigation Services
- Information Services
- Data Management Services
- Notification Services

IAFIS is a large, widely-distributed computer system. It includes more than 700 individual workstations, which support the ten-print and document service providers, latent specialists, and system administrators and operators. These workstations are distributed within Clarksburg and Fairmont, WV; Quantico, VA; Dover, DE; and Washington, D.C. facilities. The system in-

cludes a communications facility with multiple local area networks (LANs) and interfaces with three wide area networks (WANs): the CJIS WAN, the NCIC communications network, and the state-owned and operated The International Justice and Public Safety Information Sharing Network (Nlets).

IAFIS consists of six segments:

- Interstate Identification Index Segment (III/FBI)
- Electronic Fingerprint Conversion Segment (EFCON/FBI)
- IAFIS Data Warehouse (IDWH/FBI)
- Identification, Tasking and Networking Segment (ITN/FBI)
- Automated Fingerprint Identification System Segment (AFIS/FBI)[1]
- interim Data Sharing Model (iDSM/FBI)

The support services, SMC, UFB, CJIS WAN, iDSM/DHS and Card Scanning Service (CSS), were developed to support IAFIS.

1.3 Definitions

A complete list of definitions are contained in the IAFIS Acronym List and Glossary document available in the CJIS CM Library.

All data element and data aggregate definitions are found in the IAFIS Message Definition Database (MDD).

[1]This document uses the acronym AFIS to refer to an automated fingerprint identification system of any type. AFIS/FBI refers to the AFIS developed by Lockheed Martin, Inc. for the FBI. Although the FBI named AFIS/FBI as a system, it is a segment of the IAFIS.

2 APPLICABLE DOCUMENTS

2.1 CJIS Documents

a. IAFIS-RS-0010(V8), IAFIS System Requirements Definition (SRD), dated 4/1/99.
b. IAFIS Concept of Operations (ConOps), 2/17/93.
c. CJIS Documentation Plan, 5/10/95.
d. CJIS-RS-00509(V2), CJIS Technical Architecture, 2/11/98.
e. IAFIS FOC Architecture, 1/3/94.
f. CJIS Data Dictionary, 4/22/93.
g. Reserved.
h. CJIS Disposition Submission Via Machine Readable Data, 5/1/93.
i. CJIS Subject Search Specification Via Machine Readable Data, 11/91.
j. CJIS Expungement Submission Via Machine Readable Data, November 1995.
k. CJIS User Fee Billing Via Machine Readable Data, 9/94.
l. CJIS Federal User Fee Billing Via Machine Readable Data, 8/94.
m. IAFIS Filtering Rules, 4/99.

2.2 Other Documents

a. Identification Division Interstate Identification Index Program Operational and Technical Manual Revision through 8/1/94.
b. National Crime Information Center (NCIC) 2000 System Requirements, Attachment 1, 3/19/93.
c. National Law Enforcement Telecommunications Systems Users Guide—Revision July 1, 1991.
d. IAFIS-RS-2000(V2R1), Requirements Build Allocation, August 30, 1999.
e. Interim Data Sharing Model (iDSM) Project Concept of Operations, BIO-DOC_01110-1.8 dated April 18, 2006
f. Nlets User and Technical Guide, January 01, 2003
g. Data Management Plan, IDENT-TO007-DMP-IDENTiDSMDMP-0010, Dated April 18, 2006
h. DHS iDSM DMP_v1.1.doc

2.3 IAFIS Specifications

a. IAFIS-RS-0060(V8), IAFIS System Specification, dated April 1, 1999.
b. CJIS-RS-0010(V7), CJIS Electronic Fingerprint Transmission Specification (EFTS), dated January 29, 1999
c. Minimum Image Quality Requirements for Live Scan, Electronically Produced Fingerprint Cards, August 30, 1991.
d. ITN-RS-0010(V9R1), Identification Tasking and Networking/Federal Bureau of Investigation (ITN/FBI) Segment Specification, dated March 6, 1998.
e. AFIS-RS-0010(V4), Automated Fingerprint Identification System (AFIS/FBI) Segment Specification, dated February 11, 1998.
f. III-RS-0010(V9), Interstate Identification Index (III/FBI) Segment Specification, dated April 1, 1999.

2.4 Standards

a. *American National Standard for Information Systems—Data Format for Interchange of Fingerprint Information*, American National Standards Institute (ANSI/NIST-CSL 1-1993, approved 11/22/93).
b. ANSI/International Standards Organization (ISO) Documents
   1. ANSI X9.17, Key Management.
   2. ISO 7498-1—Information Processing Systems—Open System Interconnection (OSI)—Basic Reference Model.
   3. ISO 7776—Information Processing Systems—Data Communications—High Level Link Control Procedures—Description of the X.25 Link Access Procedure Balanced (LAPB)—Compatible Data Terminal Equipment Data Link Procedures.
   4. ISO 8208—Information Processing Systems—OSI—Data Communications—X.25 Packet Level Protocol (PLP) for Data Terminal Equipment.
   5. ANSI T1.606-1990—Integrated Services Digital Network (ISDN) Architectural Framework and Service Description for Frame-Relay Bearer Service
   6. ANSI T1.606a-1992—Integrated Services Digital Network (ISDN) Architectural Framework and Service Description for Frame-Relay Bearer Service (congestion management and frame size).
   7. ANSI T1.606b-1993—Integrated Services Digital Network (ISDN) Architectural Framework and Service Description for Frame-Relaying Bearer Service (network-to-network interface requirements).
   8. ANSI T1.617-1991—Integrated Services Digital Network (ISDN) Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1).
   9. ANSI T1.617a-1994—Integrated Service Digital Network (ISDN) Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling system Number 1 (DSS1) (Protocol encapsulation and PICS).
   10. ANSI T1.618-1991—Integrated Service Digital Network (ISDN) Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service.
   11. ANSI X3.139:1987—FDDI Media Access Control (MAC).

12. ANSI X3.148:1988—FDDI Physical Layer (PHY).
13. ANSI X3.186:1992—FDDI Hybrid Ring Control (HRC).
14. ANSI Standard X3.4-1977 (revised 1983)—Code for Information Interchange (ASCII).
15. Reserved.
16. RFC 791: Internet Protocol (IP).
17. RFC 792: Internet Control Message Protocol (ICMP).
18. RFC 793: Transmission Control Protocol (TCP).
19. RFC 821: Simple Mail Transfer Protocol (SMTP).
20. RFC 894: Standard for Transmission of IP datagrams over Ethernet network.
21. RFC 1813: Networked File System.
22. RFC 1042: Standard for The Transmission of IP Datagrams Over IEEE 802 Networks.
23. ANSI X3.135-1992—Database Language SQL.
24. RFC 1390: Transmission of IP and Advanced Research Projects (ARP) over Fiber Distributed Data Interface (FDDI) Networks.
25. RFC 1305: Network Time Protocol (v3)—Internet time synchronization (NTP).
26. RFC 1521: Multipurpose Internet Mail Extensions (MIME), Part One-Mechanisms for specifying and describing the format of Internet message bodies.
27. RFC 1522: Multipurpose Internet Mail Extensions (MIME), Part Two-Message Header for non-ASCII text.
28. CCITT V.35: Wide Band Modems, contained in Volume 8.1 of CCITT Standards.
29. CCITT V.24: Data communication over the telephone Network; List of definitions for Interchange Circuits between Data Terminal Equipment and Data Circuit Terminating Equipment.
30. IEEE 802.3z 1000BaseSX — 1998

Source: (ISO/IEC) International Organization for Standardization/International Electro technical Commission (IEC).
ISO TC97/SC6 Secretariat
1430 Broadway
New York, NY 10018

(ANSI)
American National Standards Institute
11 West 42nd Street
New York, NY 10036

c. Federal Information Processing Standards (FIPS) Documents
   1. FIPS PUB 46-2 Data Encryption Standard, 30 December 1993.
   2. FIPS PUB 74 Guidelines for Implementing and Using the NBS Data Encryption Standard, 1 April 1991.
   3. FIPS PUB 81 DES Modes of Operation, 2 December 1980.
   4. FIPS PUB 140-1 Security Requirements for Cryptographic Modules, 11 January 1994.
   5. FIPS PUB 107 Local Area Networks: Baseband Carrier Sense Multiple Access

with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications and Link Layer Protocol

6. FIPS PUB 146-2 Profiles for Open Systems Interconnection Technology, NIST 1994.
7. FIPS PUB 174 Federal Building Telecommunications Wiring Standard
8. FIPS PUB 175 Federal Building Standard for Telecommunications Pathway and Spaces
9. FIPS PUB 127-2 Entry SQL.

Source: National Technical Information Services
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

d. Electronic Industries Association
   1. RS-232-C—Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange, EIA-RS-232-C.
   2. Standard 802.3 Type 10BASE-T CSMA/CD Access Method and Physical Layer Specifications

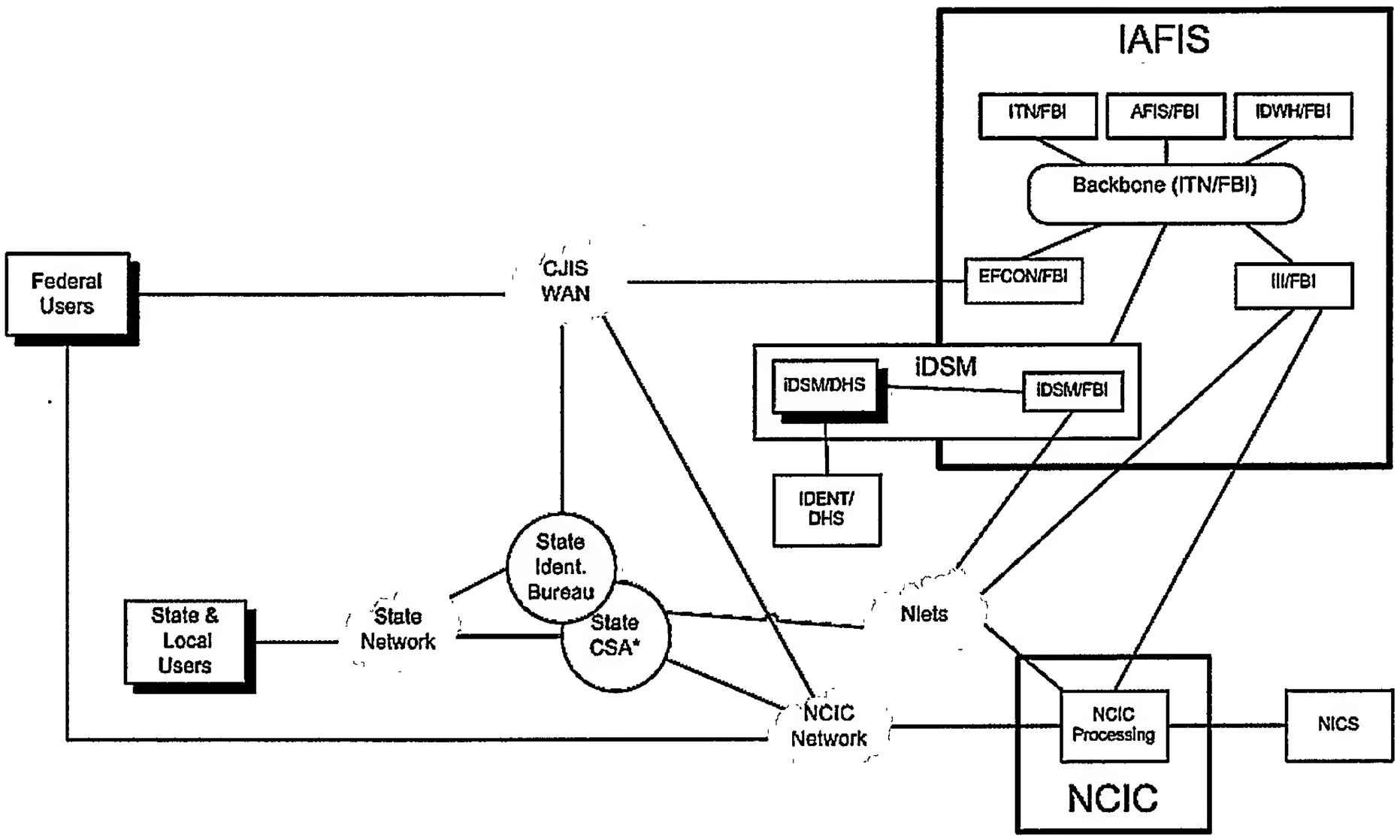
Source: EIA
Engineering Department
2001 I Street, NW
Washington, DC 20006

e. Other Documents
   1. GA27-2703—"International Business Machines (IBM) Transmission Control Component Description," IBM Systems Reference Library.
   2. GA27-3004—"General Information—Binary Synchronous Communications," IBM Systems Reference Library.

Source: IBM Corp
P.O. Box 9046
Boulder, CO 80301-9191
(Fax) 1-800-284-4721
1-800-879-2755

3 IAFIS FUNCTIONAL INTERFACES

Figure 3.1-1 IAFIS Full Operational Capability Architecture



* The State CSA is responsible for control of all state communications with the FBI

The interfaces covered by this ICD are

ITN/FBI ↔ AFIS/FBI	AFIS/FBI ↔ III/FBI
ITN/FBI ↔ III/FBI	IAFIS ↔ External
Nlets ↔ III/FBI	NCIC ↔ III/FBI
ITN/FBI ↔ iDSM/FIC	EFCON/FBI ↔ iDSM-CIPS
iDSM-CIPS ↔ DHS_VIMS	iDSM-CIMS ↔ DHS-VIPS
ITN/FBI ↔ iDSM-CIPS	iDSM/FBI ↔ Nlets/LESC

NGI-36

III/FBI ↔ iDSM-CIPS

Communication within IAFIS is through the ITN/FBI BCE.

External interfaces to the CJIS WAN are through the IAFIS FE. NCIC and Nlets connect directly to III/FBI. Communications between iDSM-CIMS and iDSM-CIPS will mirror each other, and the data will be synchronized via SMTP. All of the data between the FBI iDSM and DHS iDSM prototypes will be shared by calling upon web services that are hosted on the FBI iDSM and the DHS iDSM. Each message sent between both iDSMs will represent a transaction initiated by either IAFIS or IDENT.

The iDSM system shown in Figure 3.1-1 and discussed throughout this document is a prototype system with a finite life span. This prototype will be replaced with a permanent solution as part of the NGI program.

3.1 Summary of Processing Capabilities

The five key services provided by IAFIS are

- Identification Services
- Investigation Services
- Verification Services
- Information Services
- Notification Services
- Data Managements Services

These five key services are provided by the IAFIS segments, as described below.

EFCON/FBI provides front end communication services to IAFIS. It also provides EFTS validation and correction where necessary as well as ORI validation and verification.

The ITN/FBI segment provides ten-print processing, latent fingerprint processing, document processing, system administration, image storage and retrieval, and communications services to IAFIS, using services from the other segments as necessary. ITN/FBI ISRE is the repository for all fingerprint images in IAFIS. IAFIS segments also connect to other IAFIS segments via the ITN/FBI BCE. Hardware and protocol details of the ITN/FBI BCE interface are described in Section 4.

AFIS/FBI processes fingerprint searches and fingerprint characteristics (features) extraction. AFIS/FBI provides fingerprint search services to match ten-print and latent fingerprints against

the FBI's national fingerprint repository and provides a list of the most likely candidates. AFIS/FBI also manages remote searches from external users (i.e., criminal justice agencies) accessing IAFIS via the CJIS WAN.

III/FBI provides subject search, criminal history processing, *ad hoc* subject search, and response generation services. III/FBI will also provide criminal photo (i.e., "mug shot") storage and retrieval[2] via the Interstate Photograph System (IPS/FBI). III/FBI maintains criminal history data, including arrest, disposition, biographic, and physical data. As part of its Response Generation function and in response to Criminal History requests, III/FBI will request state-maintained criminal history data and will interface with NCIC for "Want/Flash" status checks.

All segments perform file/database maintenance functions. The *add* database maintenance function adds new data to the file/database. The *update* function replaces incorrect or old data with correct or new data in the file/database. *Delete* removes incorrect, expunged, or consolidated data from the file/database. The file/database maintenance functions are coordinated by a single segment which has been designated as the segment responsible for maintaining file/database synchronization of the data that is replicated across the IAFIS segments. For example, III/FBI is the segment responsible for the data synchronization of the databases/files (ITN/FBI Criminal Ten-Print Fingerprint Image Master File, AFIS/FBI Criminal Ten-Print Fingerprint Features Master File, etc.) which contain data replicated from the III/FBI Subject Criminal History File.

IDWH/FBI provides a user fee billing capability for IAFIS. III/FBI will regularly send data to ITN/FBI to support these capabilities.

iDSM/FBI provides a means by which to share information between IAFIS/FBI and IDENT/DHS. This interoperability effort will permit both the Department of Homeland Security (DHS) and Department of Justice (DOJ) and their users to seamlessly share identification data that is complete, accurate, current, and timely. The flow of information being shared will be multi-directional.

These functions are described in detail in the IAFIS/FBI System Specification.

3.2 Intersegment Transaction Management

Three application-level intersegment transaction protocols will be supported by the IAFIS segments. These application-level protocols overlay the existing message definitions and are the mechanisms provided for coordinating the service requests between segments (which always

---

[2] MRD input is not allowed for criminal subject photo data.

consist of a "request" message and, normally, a "response" message). The intersegment transaction protocol to be used for a given service request will be decided by the segment contractors and imbedded in the IAFIS Header. The responding segment then uses this header information to validate the service request.

All of the data between the FBI-iDSM and DHS-iDSM and the FBI-iDSM and the DHS_LESC will be shared by calling upon web services that are hosted on the FBI iDSM and the DHS iDSM.

Associated with each of the intersegment transaction protocols are restart responsibility, time-out strategies, and error/exception handling. Section 3.2.1 describes the basic intersegment transaction protocols and the appropriate use of each of the protocols. Sections 3.2.2, 3.2.3, and 3.2.4 describe the restart responsibilities, time-out strategies, and error/exception handling associated with each of the intersegment transaction protocols. The text and figures provided in these sections are examples and are not intended to imply a segment design. Appendix I describes the details of the iDSM web services

3.2.1 Intersegment Transaction Protocols

The three different protocol styles will be referred to as the Immediate Response (IR) protocol, the Queued Response (KR) protocol, and the No Response (NR) protocol.

- The IR protocol does not add any additional "handshaking" messages to the request/response pair and is best suited for “fast” transactions where the requesting segment is waiting for an immediate response. An example is a latent service provider’s subject search request.
- The KR protocol adds "handshaking" messages to the intersegment transaction and is best suited for longer intersegment transactions where no reply/data is expected or an immediate reply/data is not expected. Examples of this type of service request are AFIS/FBI searches and ITN/FBI Image retrievals.
- The No Response protocol is used when the requesting segment does not need anything in return from the accepting segment. One “handshaking” message indicates that the accepting segment has accepted the request. Examples of this type of service request are AFIS/FBI requests to III/FBI to generate and send EBTS responses.

3.2.1.1 Immediate Response Protocol

Figure 3.2.1.1-1 shows the basic IR protocol. No additional "handshaking" messages above the actual request message and reply/data message are in this protocol. Use of the IR protocol requires that the requesting segment retains the responsibility for "properly processing" the intersegment transaction. (i.e.: Any restart of the intersegment transaction is the responsibility of the requesting segment.) In some cases, the reply/data message transmitted by the responding segment will be a simple answer that the request has been completed successfully (or not). In other

cases, returned data is included in the reply/data message.

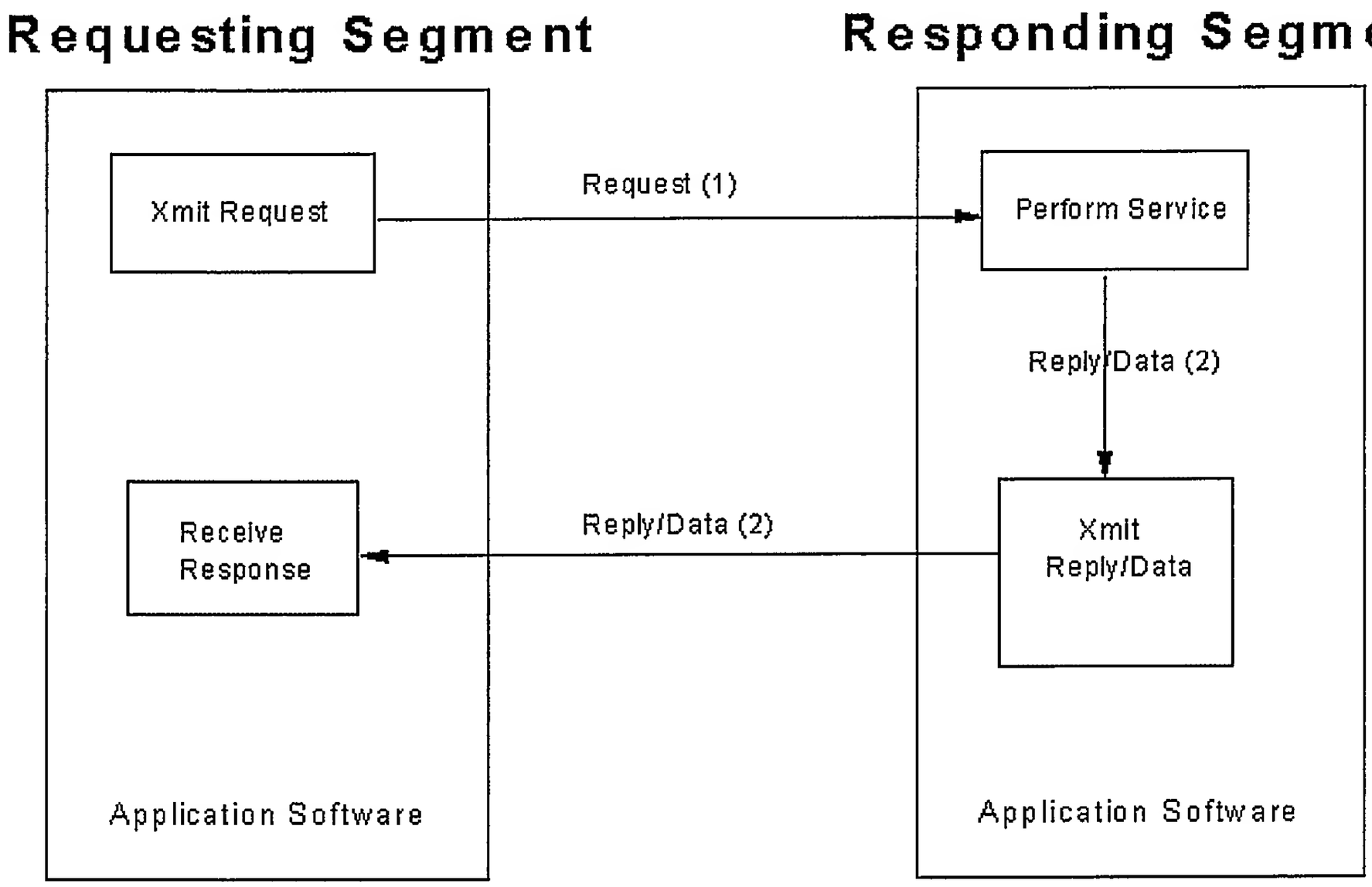


Figure 3.2.1.1-1 Basic Immediate Response (IR) Intersegment Service Request Protocol

This intersegment service request protocol is not efficient or effective for all IAFIS transactions. In particular, the IR protocol is not efficient for lengthy service requests. In these cases, the time delays, minutes to hours, complicate the recovery process for overdue answers which will be arriving late or not at all.

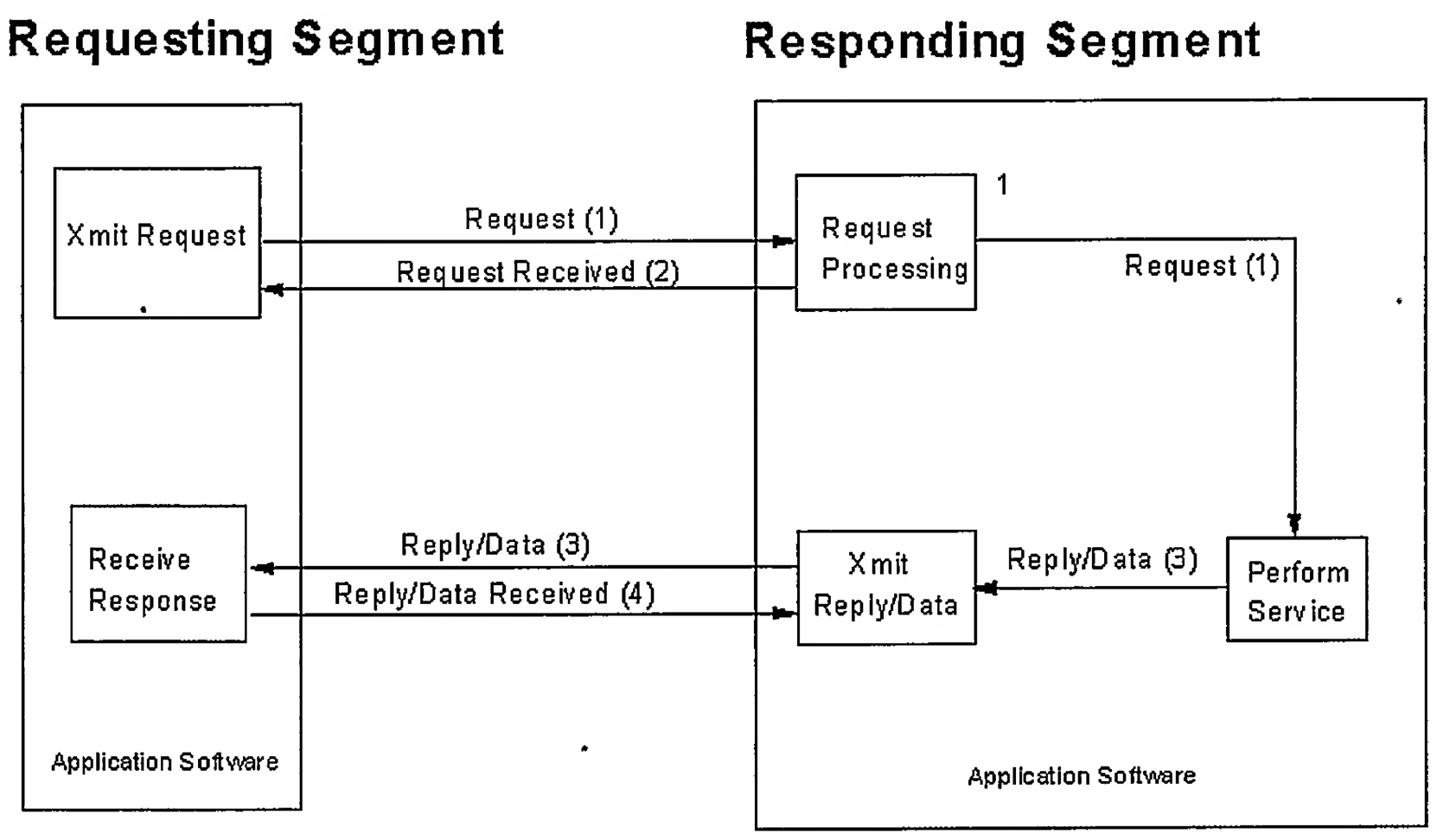
A straightforward way of resolving these kinds of problems is to make use of a second type of intersegment service request protocol that permits segments to reliably hand-off intersegment transaction responsibility to responding segments.

3.2.1.2 Queued Response Protocol

Figure 3.2.1.2-1 shows the basic KR protocol. In this protocol, "handshaking" messages are added to the normal request/response message pair to ensure that the responding segment received and understood the original request and that the requesting segment received the reply/data. In this protocol, the requesting segment transfers responsibility for "properly processing" to the res-

ponding segment until receipt of the reply/data (restart responsibility is passed from the requesting segment to the responding segment). This protocol is best suited when the reply/data is not expected immediately (e.g.: ad-hoc searches). This protocol should be used for service requests which take a long time to complete (i.e.: minutes to hours).

In the KR protocol, once the request is received and the message is validated, the responding segment sends a "Request Received" message accepting responsibility for "properly processing" the request. Essentially the responding segment is replying that it "has received the request, understood the request, will perform the request, and will tell the requesting segment when the service is done." When the responding segment finishes processing the request, it sends a second message to the requesting segment providing the answer along with any needed data. To ensure that the transaction processing is properly completed, the requesting segment must transmit a final message acknowledging receipt of the reply/data.



1. In subsequent KR figures, i.e. Figures 5, 7, and 9, this block will be expanded to show additional functionality

Figure 3.2.1.2-1 Basic Queued Response (KR) Intersegment Service Request Protocol

To meet throughput and response time requirements when transferring large messages, the KR protocol supports an optional Retrieve File step as shown in Figure 3.2.1.2-2. Prior to transmitting the request, the requesting segment places the Data File onto a previously configured Network File System (NFS) remote-mounted disk. During Request Processing, the responding segment retrieves the file identified within the request message from the requesting segment. The responding segment will no longer have access to the file once it has returned the associated Request Received response. Internal Ten-Print Submission processing provides an example of the use of this protocol.

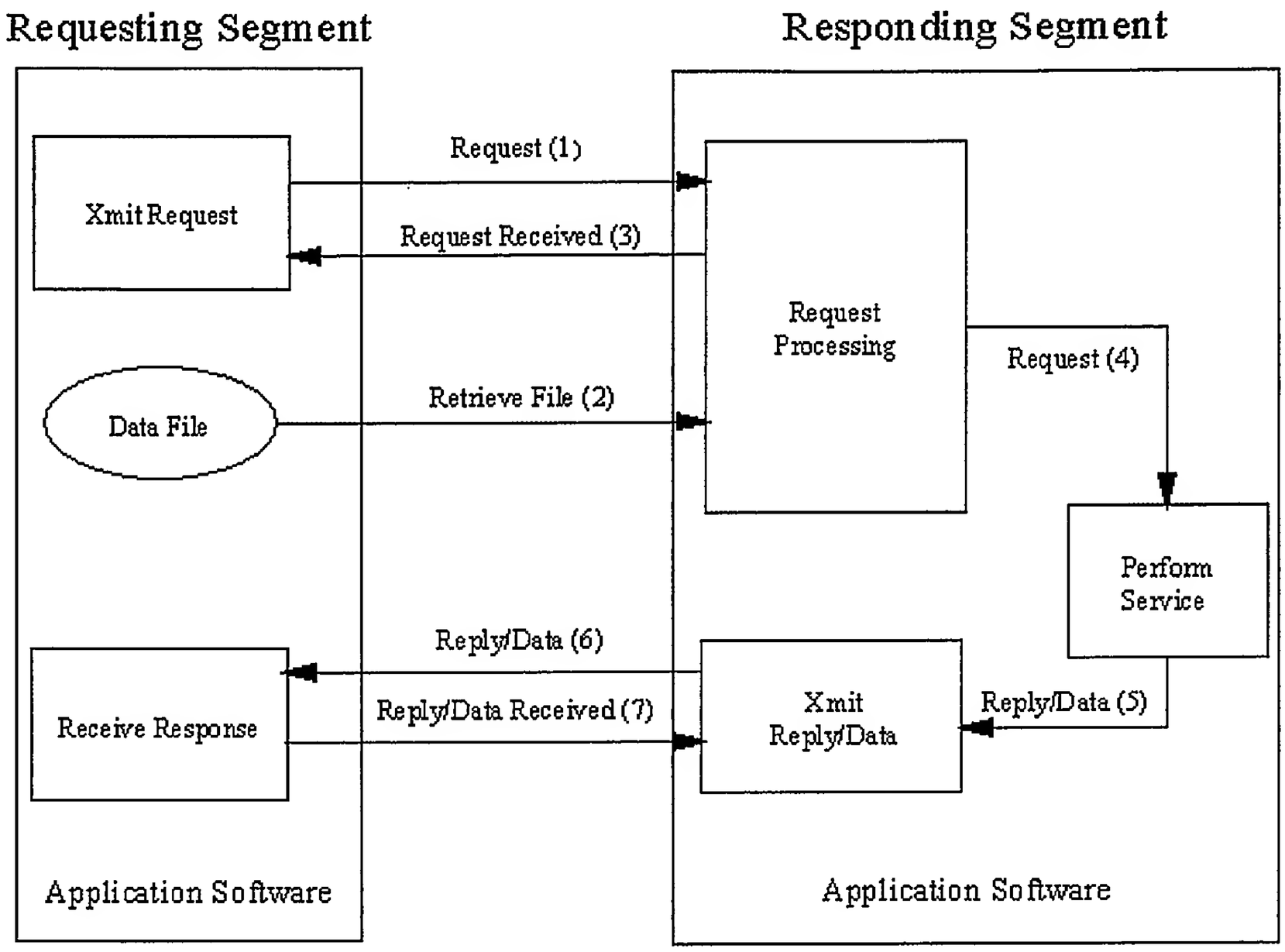


Figure 3.2.1.2-2 Basic Queued Response (KR) Intersegment Service Request Protocol with File Retrieve Options

3.2.1.3 No Response Protocol

Figure 3.2.1.3-1 shows the basic No Response (NR) protocol. There is only one transfer of data from the requesting segment to the accepting segment. Once the request is received and the message validated, the accepting segment sends a "Request Received" message accepting responsibility for "properly processing" the request. However, unlike the Queued Response protocol, the accepting segment will not notify the requesting segment when the service is done. The requesting segment is finished with the transaction when the accepting segment agrees to take the request. At that time, the accepting segment acquires full responsibility for completing the processing of the transaction.

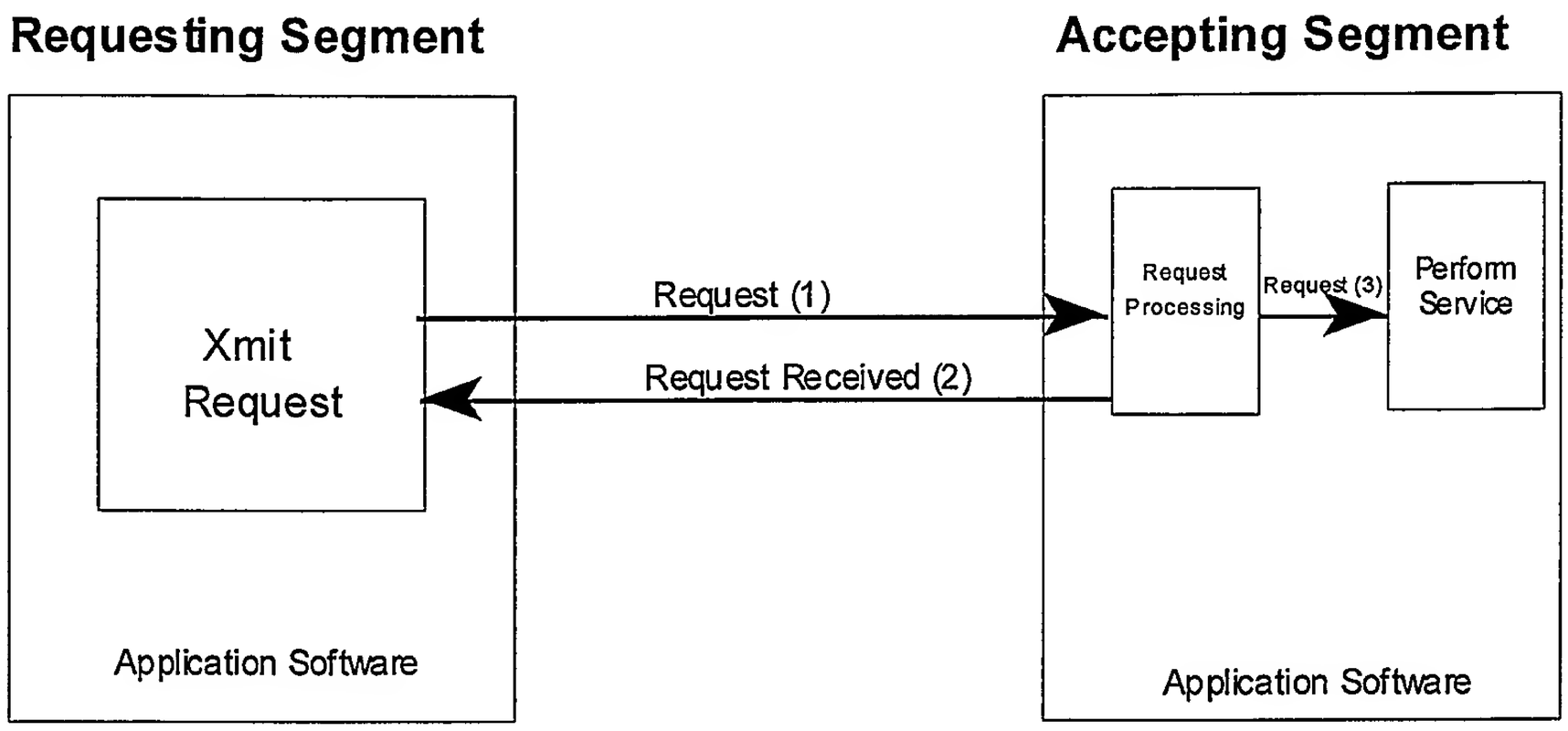


Figure 3.2.1.3-1 Basic No Response Intersegment Service Request Protocol

The NR protocol also supports an optional Retrieve File step during Request Processing identical to that supported by the KR protocol, shown in Figure 3.2.1.3-2. Prior to transmitting the request, the requesting segment places the Data File onto a previously configured NFS remote-mounted disk. During Request Processing, the accepting segment retrieves the file identified within the request message from the requesting segment prior to responding with the Request Received. At that time, the responding segment no longer has access to the data file. Remote Ten-Print Search processing provides an example of the use of this option within the NR protocol.

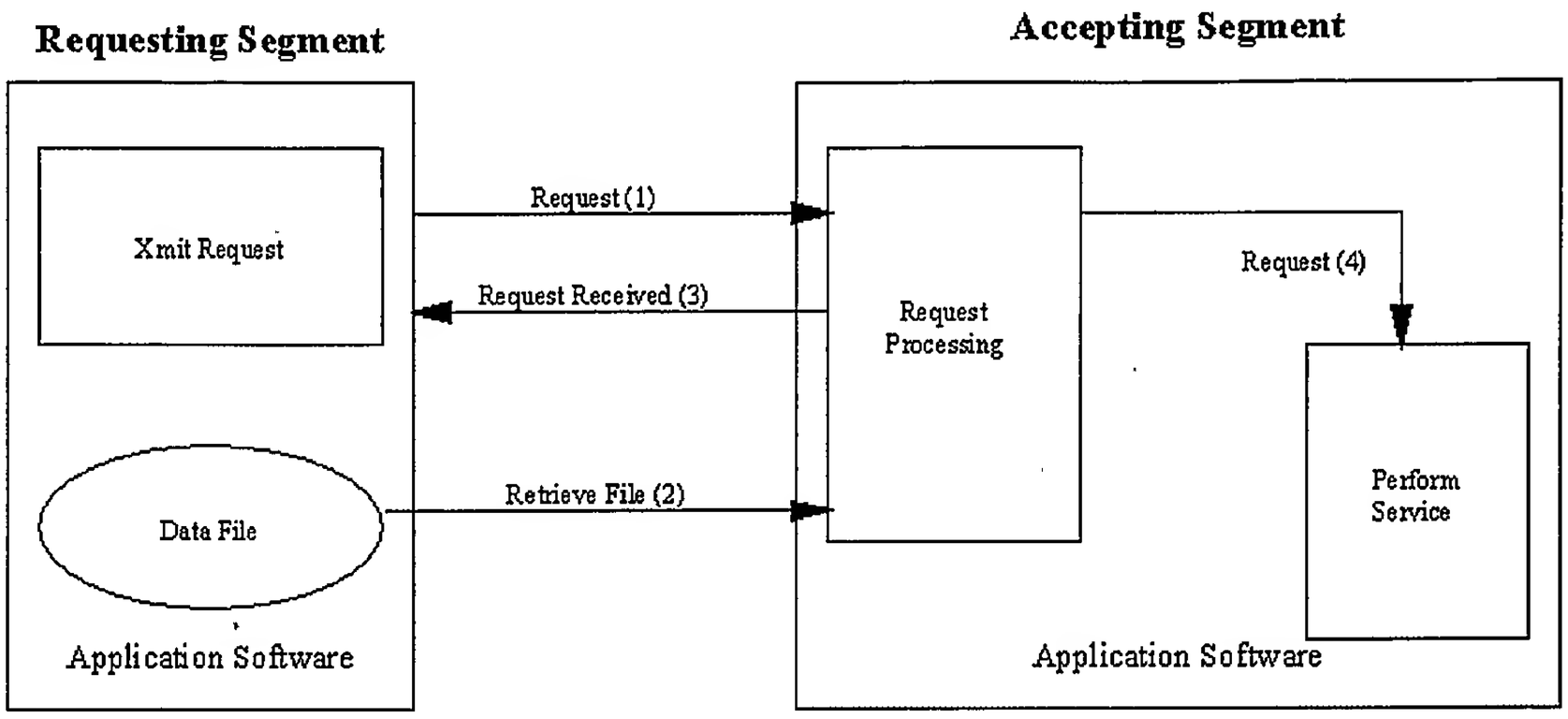


Figure 3.2.1.3-2 Basic No Response (NR) Intersegment Service Request Protocol with File Retrieve Options

3.2.2 Restart Implications

Each type of intersegment transaction protocol has different restart implications. Restart responsibility is coordinated between the two segments as described in the following paragraphs.

When the IR protocol is used, the requesting segment retains the responsibility for ensuring that the intersegment transaction is properly processed. If a request is not satisfied for any reason, the requesting segment is responsible for initiating any restart of the request, if appropriate.

When the KR protocol is used, the responsibility for restart is temporarily shifted from the requesting segment to the responding segment as shown in Figure 3.2.2-1.

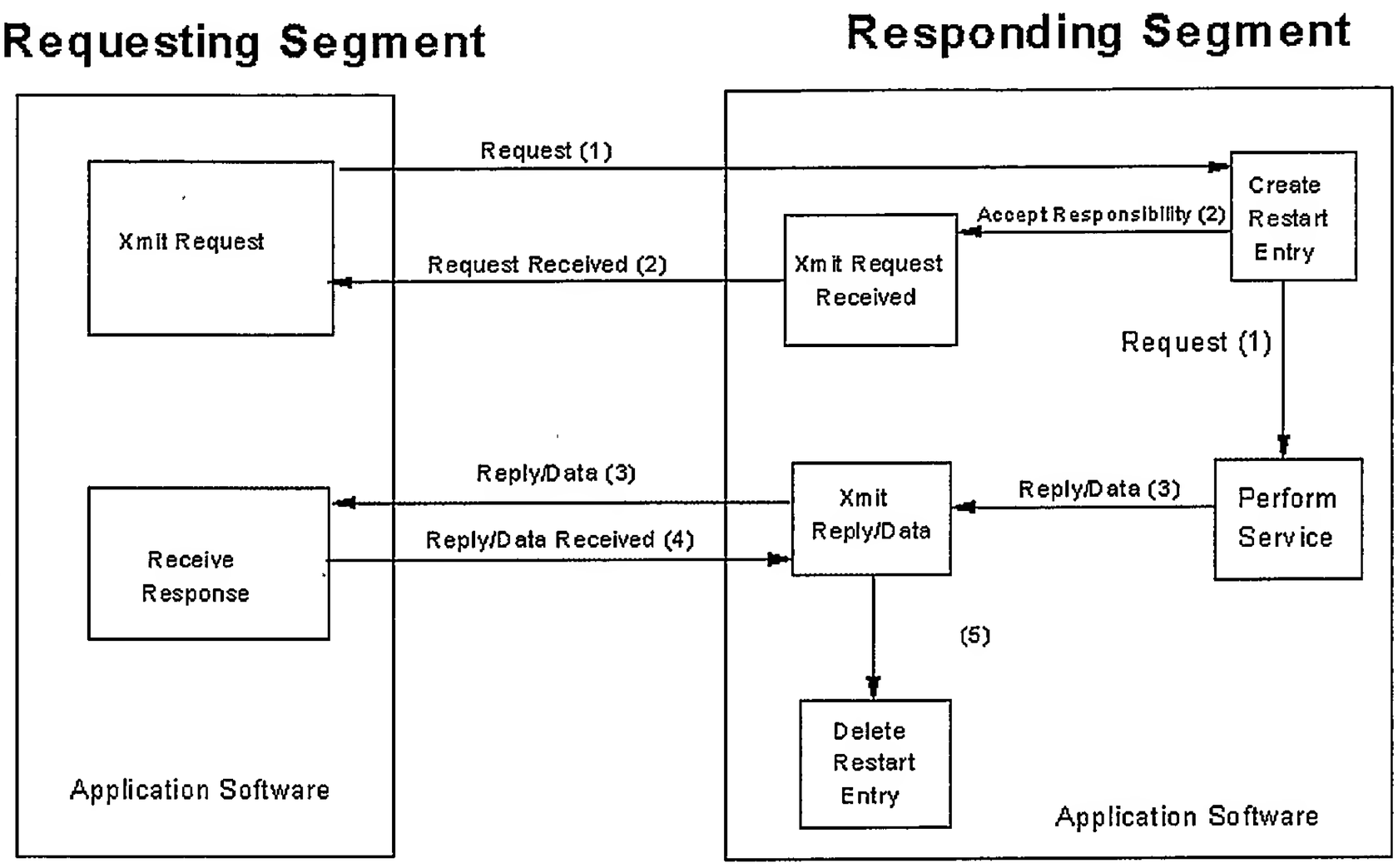


Figure 3.2.2-1 Restart Responsibilities Associated With Queued Response

When the KR protocol is used, intersegment transaction completion, recovery, and restart responsibilities initially reside with the requesting segment. These responsibilities shift to the responding segment once the "Request Received" message has been sent. As shown in Figure 1.7-4, one of the first things the responding segment does once it has received a KR request is to create a restart entry. With the restart entry established, the responding segment proceeds to transmit the "Request Received" message to the requesting segment and perform the requested service. Upon completion of the service, the responding segment sends the reply/data to the requesting segment. Once the reply/data message is received by the requesting segment, it transmits an acknowledgment and reassumes its original responsibilities. Once the responding segment receives acknowledgment that the reply/data message was received, it deletes its restart entry and relinquishes its responsibilities.

When the No Response protocol is used, recovery and restart responsibilities initially reside with the requesting segment. These responsibilities shift to the accepting segment once the "Request Received" message has been sent. Like the Queued Response protocol, the accepting segment creates a restart entry. But, in the case of the No Response protocol, the requesting segment never resumes responsibility for the system transaction. When the receiving segment completes the request, it is the receiving segment's responsibility to delete the restart entry.

3.2.3 Response Time and Time-Out Implications

Each type of intersegment transaction protocol has different response time and time-out implications. In the IR and KR intersegment transaction protocols, response-time expectations and time-outs are coordinated between the two segments. This coordination is described in the following paragraphs.

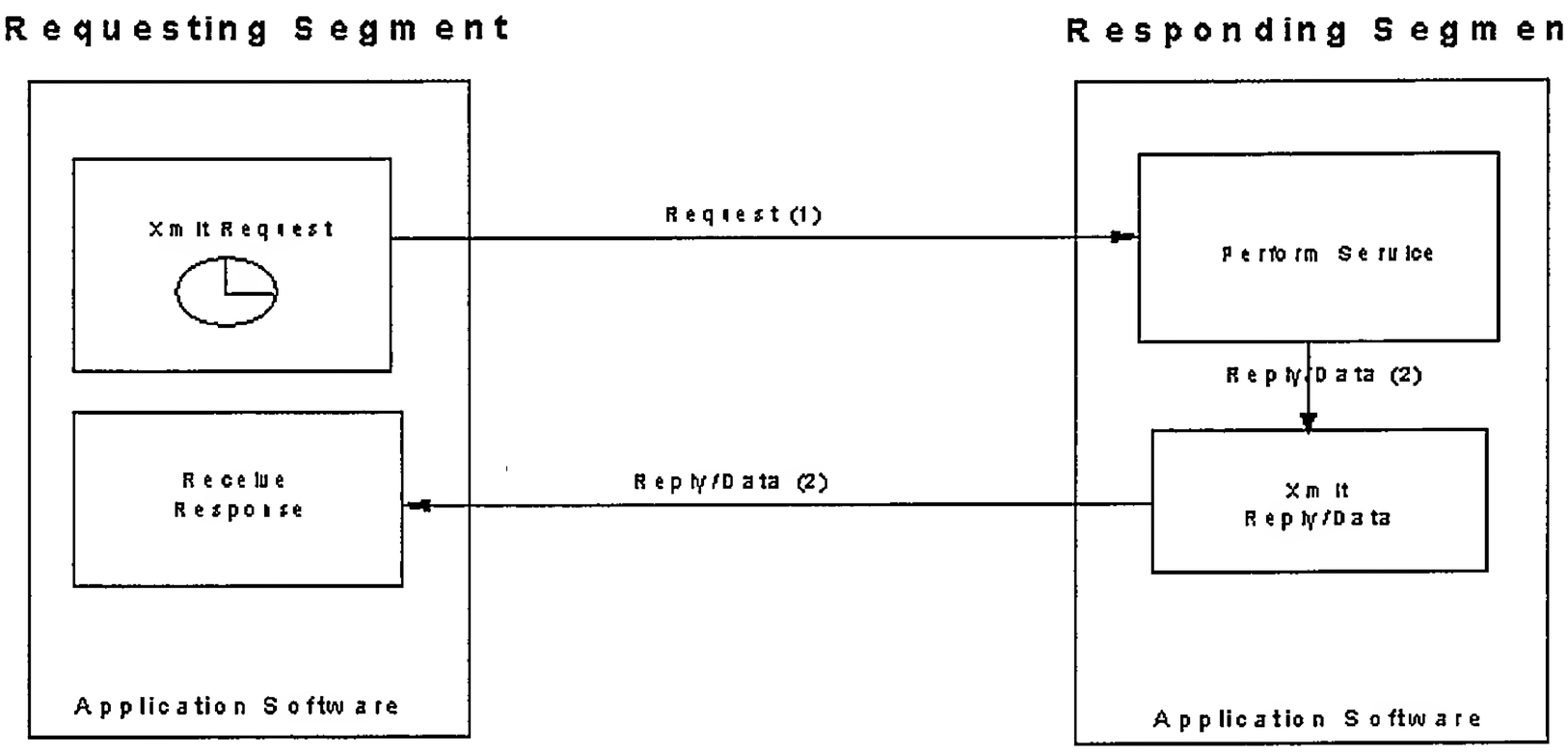


Figure 3.2.3-1 Immediate Request Protocol With Response Time-Out Clock Added

For both IR and KR protocol types to function properly, one or more time-out clocks must be used. Figure 3.2.3-1, depicting the IR protocol, uses a clock in the Xmit Request block to show that the requesting segment must establish a time-out value for deciding when an outstanding request will be declared overdue (i.e.: a reply/data message has not been received). A response time-out will frequently be the initial event in a restart or recovery sequence within the requesting segment.

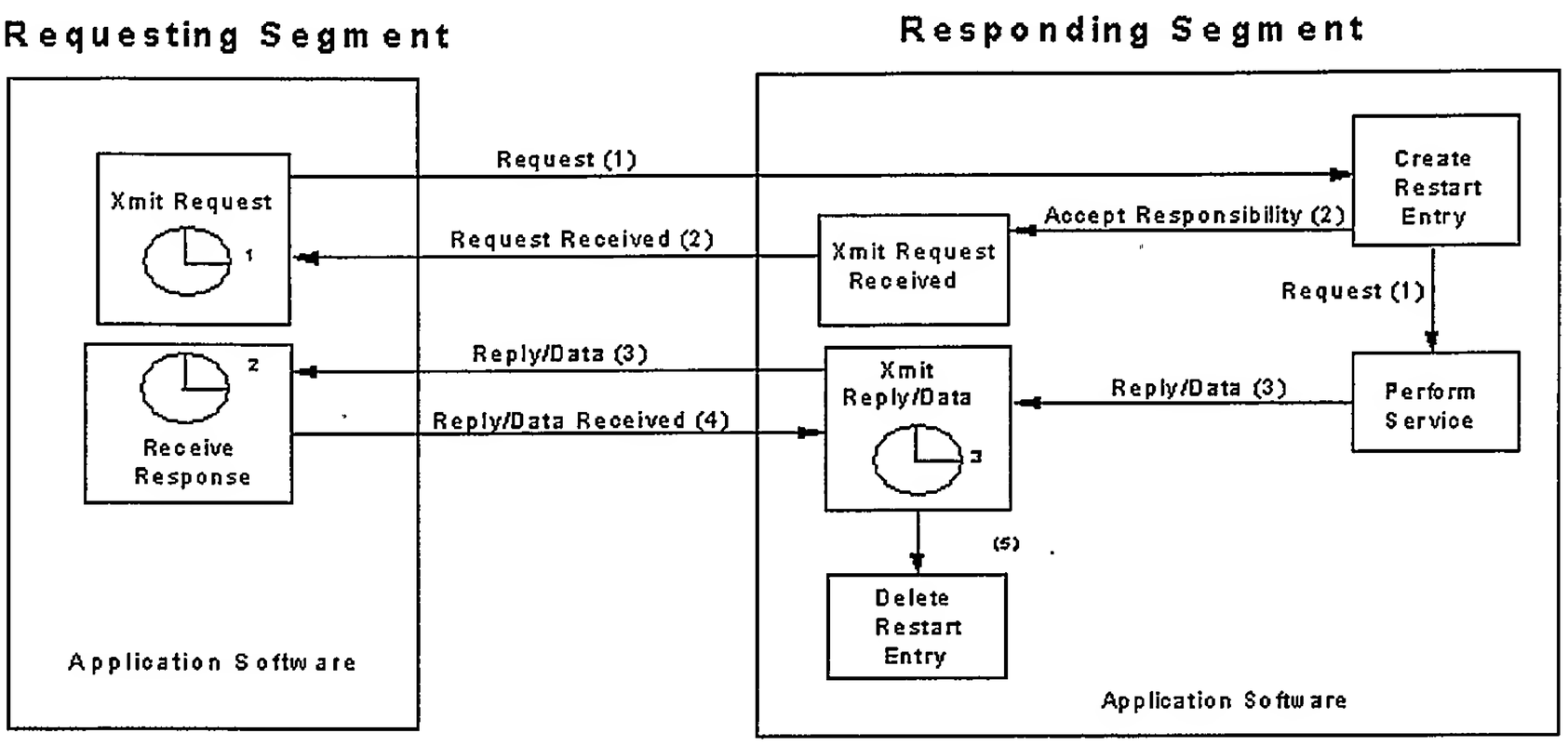


Figure 3.2.3-2. Queued Response Protocol With Response Time-Out Clocks Added

Figure 3.2.3-2 shows a comparable set of time-out clocks for the KR protocol. Three time-out clocks are shown here because intersegment transaction recovery and restart responsibility shifts back and forth between the two segments.

The first clock times out if the "Request Received" message is overdue. The second clock times out if the "Reply/Data" message is overdue, and the third clock times out if the "Reply/Data Received" message is overdue. In general, the first and third clock time-out values should always be relatively short because the messages they monitor should always arrive shortly after the request unless a problem has occurred.

The second clock's time-out value will be message- and scenario-dependent. Functionally, it is a method to detect the fact that a reply was expected and never received. Because the responding segment is responsible for the transaction during this time and because the requesting segment is not responsible for recovery or restart, the system designers may find it useful to set its time-out to a relatively large value compared to the expected response time. For example, assume that IAFIS decides to use the KR protocol for ten-print searches required for a ten-print submission. The AFIS/FBI segment has various response times (e.g.: 15 minutes, 30 minutes) for its responses depending on the priority of the search request. ITN/FBI might choose to set clock two's time-out value to several hours for the system transaction priorities corresponding to a 24-hour ten-print search submission to ensure that AFIS/FBI has ample time to recover and restart requests when it experiences internal problems. This strategy minimizes the involvement of the ITN/FBI segment in AFIS/FBI problems without necessarily compromising end-to-end response times. It should be noted here, that the responding segment should send an error message by the designated time if it cannot successfully perform the service by that time. This will not, however, pass restart responsibility back to the requesting segment.

The second clock's time-out value is imbedded in the IAFIS header so that the responding segment knows when the reply/data will be treated as overdue. In addition, the KR protocol allows the responding segment to return an expected completion time if the responding segment cannot do the request within the specified time. The requesting segment would then reset the second clock, and the restart responsibility remains with the responding segment. This supports coordination between the segments if the responding segment is over-loaded.

In the No Response protocol, the only time-out value that matters is the time required for the accepting segment to send the "Request Received" message to the requesting segment. It is the responsibility of the requesting segment to determine that value.

3.2.4 Web Services

Within iDSM/FBI, the web servers will reside in two locations; the CIPS and the CIMS. Each web server will reside on the same physical server as the application server to efficiently leverage iDSM hardware. The servers that process the web services requests will interface with the DHS VIMS and VIPS. These web services are described in greater detail in Appendix I.

3.2.5 Flat File and Image Retrieval

iDSM/FBI will acquire candidate data from IAFIS/FBI nightly via a flat file transfer from III/FBI. III/FBI will generate a delimited file by querying its database nightly, for all data that should be shared with an external agency. The file that is sent from III, via SCP, provides the FNU, the name, type (TYP) field indicating whether this is Wants/Warrants or KST data, date/time stamp (DTS), date of birth, place of birth, gender, Originating Agency Identifier (ORI), the NIC number (NIC), and the Case number (OCA) when dealing with Wants/Warrants. Details of each field are available in the following sections.

Based on the contents of this file, iDSM/FBI will determine what candidates need to be added to access its shared data repository. These FNUs will be used to retrieve images from the ITN/FBI FIMF using a SQLNet connection. The images will then be passed to CIPS using SMTP protocol, to be added to or removed from the repository. Details of this message (A3310) can be found in the MDD.

3.2.5.1 Data Assembly Characteristics & Field/Element Definition

Table 3-1 shows the data that is included in the delimited sync file.

Table 3-1: Incoming Sync Data Sharing Notification Format

Field Name	Description	Type	Length
FNU	FBI Number (Nine Alphanumeric Characters)	String	9
NAM	Master Name of the IAFIS record	String	30
DOB	First Date of Birth (CCYYMMDD) of the IAFIS record	String	8
SEX	Gender	String	1
ORI	Originating Agency Identifier of the wanting agency	String	9
NIC	NIC number when dealing with Wants/Warrants	String	10
OCA	Case number when dealing with Wants/Warrants	String	20
POB	Place of Birth	String	2
TYP	Type of data being shared • WW – Wants/Warrants data • K1 – KST data	String	2

3.2.6 Exception and Error Handling

The final feature that is needed for the intersegment transaction protocols to function is exception and error handling. Two main types of intersegment transaction exceptions/errors can occur with the second type divided into three subclasses as shown below:

1) "Invalid Request": This type of error occurs when the data validation of the original request fails. The system-wide strategy for request validation is to have both the requesting and responding segments validate the request. Having the requesting segment perform validation ensures that any errors are detected and corrected as quickly and as close to the source as possible. In addition, requester validation minimizes the number of invalid requests that are eventually rejected by the responding segment. Validation is done within the responding segment to ensure that it does not attempt to process an invalid request.
2) "Unable to Process, There is a Problem": This class of exception or error is different from the invalid request because the request message passed the validation check but the service did not complete successfully. This type of error is broken down further because the actions of the requesting segment may be different for each subclass.
   - The "Responding Segment Problem" subclass should be interpreted by the requesting segment to mean that the responding segment is unable to satisfy the request at this time but should be able to later. An example of this type of error would be when the AFIS/FBI segment receives and queues a latent search only to

find that its latent search capability fails before the job can be completed. In these cases, once the responding segment corrects the problem, the responding segment will satisfy the original request.

- The "Requesting Segment Problem" subclass indicates that the responding segment can never do the request exactly as it was sent. Although the request passed the validation check, some type of problem with the original request still requires correction by the requesting segment. An example of this type of problem would be an ITN/FBI file update request sent to III/FBI where III/FBI finds that no available fields are left to store the alias information in the request. The responding segment will never be able to process the request until an appropriate change is made to the request message by the requesting segment.
- The "Mutual Problem" subclass indicates that a data consistency problem was uncovered while trying to process the request. This problem subclass requires manual intervention by segment operators or system administrators of both segments involved to determine which data is in error. An example of this condition is when a data synchronization problem occurs. III/FBI has data for the subject, but ISRE does not have the corresponding ITN/FBI image. The segment operators and system administrators must then use the tools provided for the segments to investigate and correct the discrepancy while the request remains on "hold" pending the resolution of the problem.

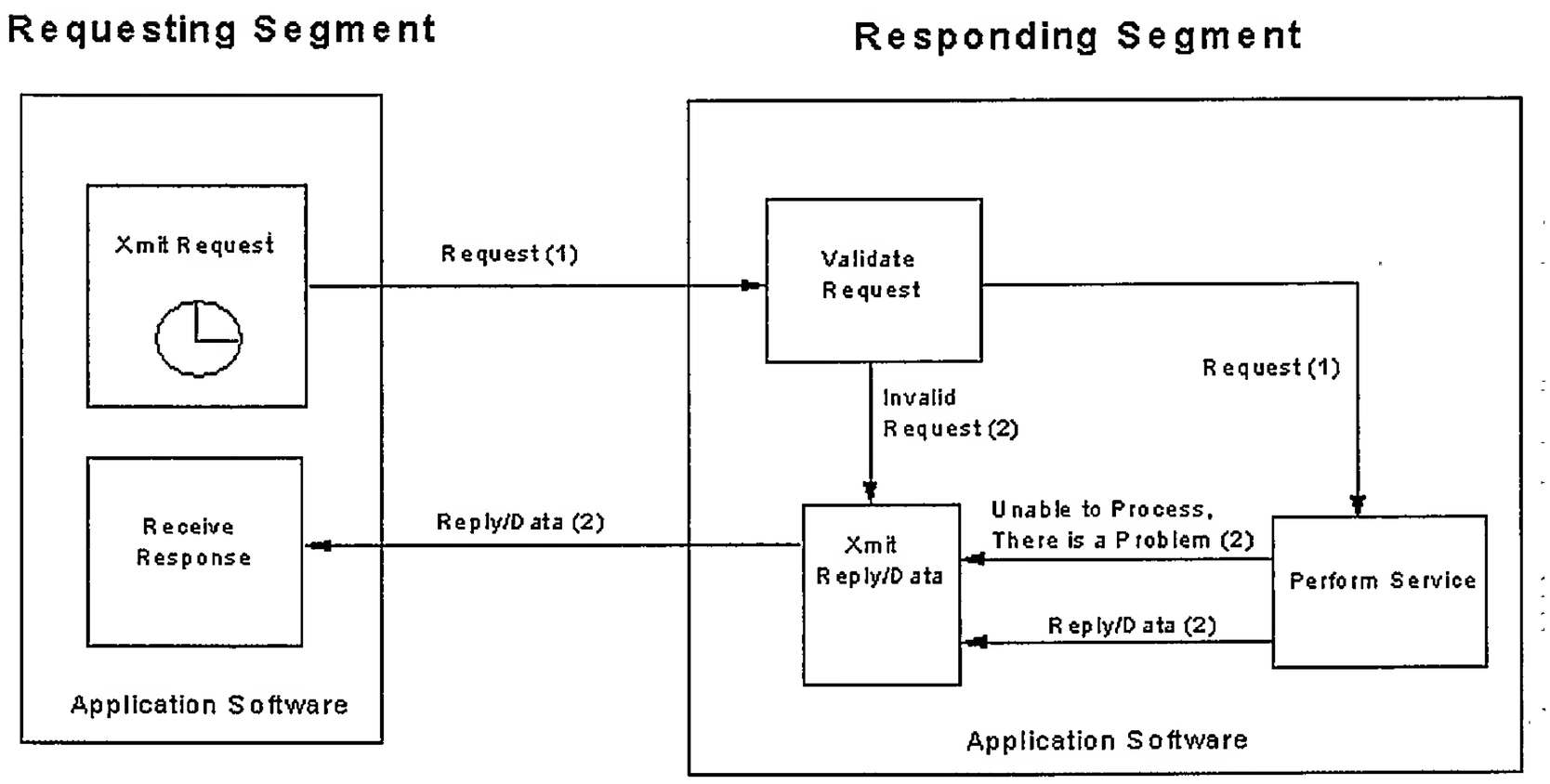


Figure 3.2.6-1 Complete Immediate Response Protocol Including Exception and Error Handling

Figure 3.2.6-1 shows the IR protocol diagram as it was shown in Figure 3.2.1.1-1 with the addition of the two major exception and error-handling data flows. Invalid Request messages are transmitted to the receiver as the reply to the original request as shown by the parenthesized two. The second type of exception or error that can occur, the "Unable to Process, There is a Problem" message, is also returned as the reply to the original request.

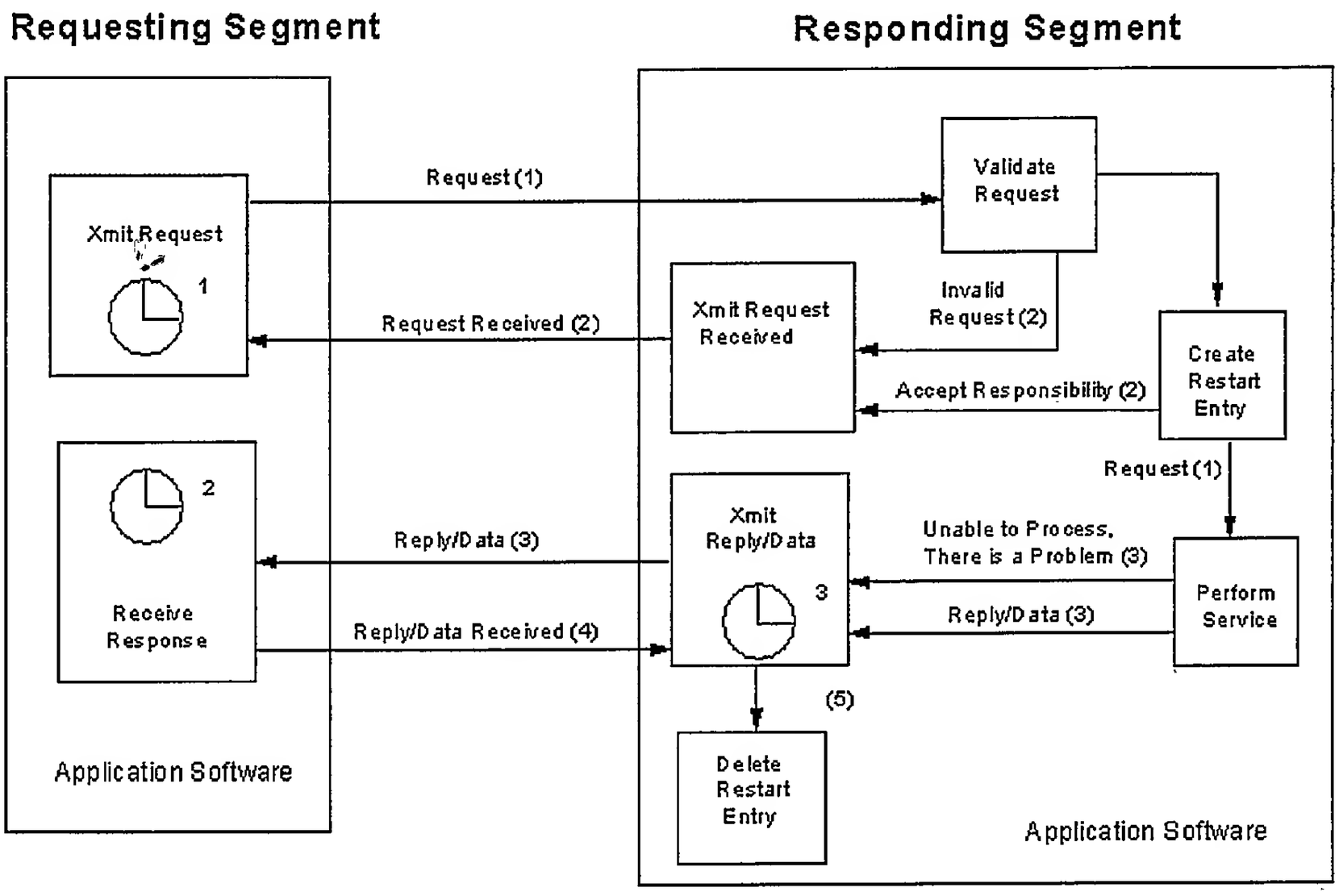


Figure 3.2.6-2 Complete Queued Response Protocol Including Exception and Errror Handling

Figure 3.2.6-2 shows the equivalent picture for the KR protocol. In the KR protocol, the responding segment validates the request message prior to accepting restart responsibility and, if the message does not pass the validation check, sends the "Invalid Request" message in lieu of the "Request Received" message. This ensures that the requesting segment is told immediately if an error is in the request message and the responding segment does not assume restart responsibility for an intersegment transaction it cannot perform.

The "Unable to Process, Responding Segment Problem" message is transmitted as an informational message to the requesting segment when the problem is the responding segments, not in lieu of the "Reply/Data" message. It should be noted here that, in the case of "Unable to Process, Responding Segment Problem" the responding segment retains the responsibility for fixing the problem until the elapsed time exceeds the time out value in the IAFIS header. In other words, the responding segment should try to correct the problem within the allotted time and only sends the "Unable to Process, Responding Segment Problem" message if the problem cannot be fixed before the requesting segment's second clock time-out value is exhausted.

The "Unable to Process, Requesting Segment Problem" message is transmitted in lieu of the "Reply/Data" message when the problem is the requesting segments. The responding segment does not retain any responsibility for the message, the requesting segment must resend the message in it's entirety when the problem is corrected.

The "Unable to Process, Mutual Problem" message is transmitted when a problem co-exists in both segments' problem. An example would be the detection of an out-of-synch condition. The responding segment retains the restart responsibility for the message pending the resolution by the segment operators and systems administrators. The requesting segment suspends the time-out clock until the problem is corrected.

Error handling for the No Response protocol is simplified by the fact that, once the accepting segment accepts responsibility for the system transaction, no other segment needs to know about any errors or exceptions. Only the "Invalid Request" message will be sent to the requesting segment. If so, it is sent in lieu of the "Request Received" message, and the requesting segment retains responsibility for the system transaction.

When the file retrieval option is used in the KR and NR protocols, the responding segment confirms the availability of the remote mounted data file indicated in the Request message and retrieves the file during its Validate Request process. If an error occurs during this process, the responding segment will transmit the "Invalid Request" message in lieu of the "Request Received" message. The responding segment does not retain any responsibility for the message.

To meet throughput requirements, the responding segment may transfer the file using file copy configured for asynchronous write protocol to the destination file. If the copied file is subsequently lost or determined to be corrupt, whether due to the segment failure or to errors in the source file, the responding segment will initiate error processing as described within section 4.9, Error Processing and Exception Handling, according to the protocol of the associated message.

3.3 Special Stop Filtering

The intersegment messages in the MDD contain filtering elements as necessary to accomplish filtering. While the ICD contains the required data flows to accomplish filtering, as well as some comments describing intrasegment filtering/review actions, the data flow sequencing and notes are not intended to state all the required filtering and review actions. For example, for certain circumstances in response to the Subject Search (A1030) and the Service Provider Subject Search (A1032) from ITN/FBI, III/FBI performs filtering (either for AUD "T" subjects or all special stop subjects) and provides filtering information in the service response. This is not explicitly stated in the sequencing and notes, although the MDD messages provide for that information. Instead, this information is found in the *"IAFIS Filtering Rules."*

III/FBI and ITN/FBI are the main IAFIS segments involved in special stop processing. III/FBI is the IAFIS segment which filters transactions. ITN/FBI provides most of the functionality to allow Special Stops service providers to perform their work. ITN/FBI must also automatically reroute transactions to allow for special stop processing.

3.4 IAFIS—External Interfaces

The EFCON/FBI communicates with external entities via the ITN/FBI BCE and the IAFIS/FBI FE. III/FBI interfaces with the NCIC Front-End (FE), and Nlets. The NCIC FE and CJIS WAN provide criminal justice agencies (Federal, state, and local) access to IAFIS services. Nlets provides an interface with the states' systems for receiving administrative messages and states' criminal history records and for monitoring states' responses to requests for criminal records.

The IAFIS/FBI FE provides routing and communications processing capabilities for these transactions.

Hardware and protocol details of external interfaces are found in Section 4, additional details of the ITN/FBI BCE interface are also described there.

3.5 Message Flow

Appendix B and the online MDD present IAFIS Data Flow. Note that some messages may have multiple origins and/or destinations. Details of message definition are contained in the MDD and enumerated in Appendix A. Details of physical routing of data are found in Appendix B.

4 IAFIS COMMUNICATIONS INTERFACES

The IAFIS communications interfaces described in this section provide for both internal and external connectivity for IAFIS segments and IAFIS users. All characters within IAFIS messages defined herein shall comply with the *ANSI Standard X3.4-1977 (revised 1983), American National Standard Code for Information Interchange (ASCII).* The IAFIS/FBI FE provides gateway services for all IAFIS segments to external activities, users, and services. The ITN/FBI BCE provides for internal connectivity to the IAFIS segments.

4.1 IAFIS External Communications Interfaces

4.1.1 IAFIS/FBI—CJIS WAN Interface

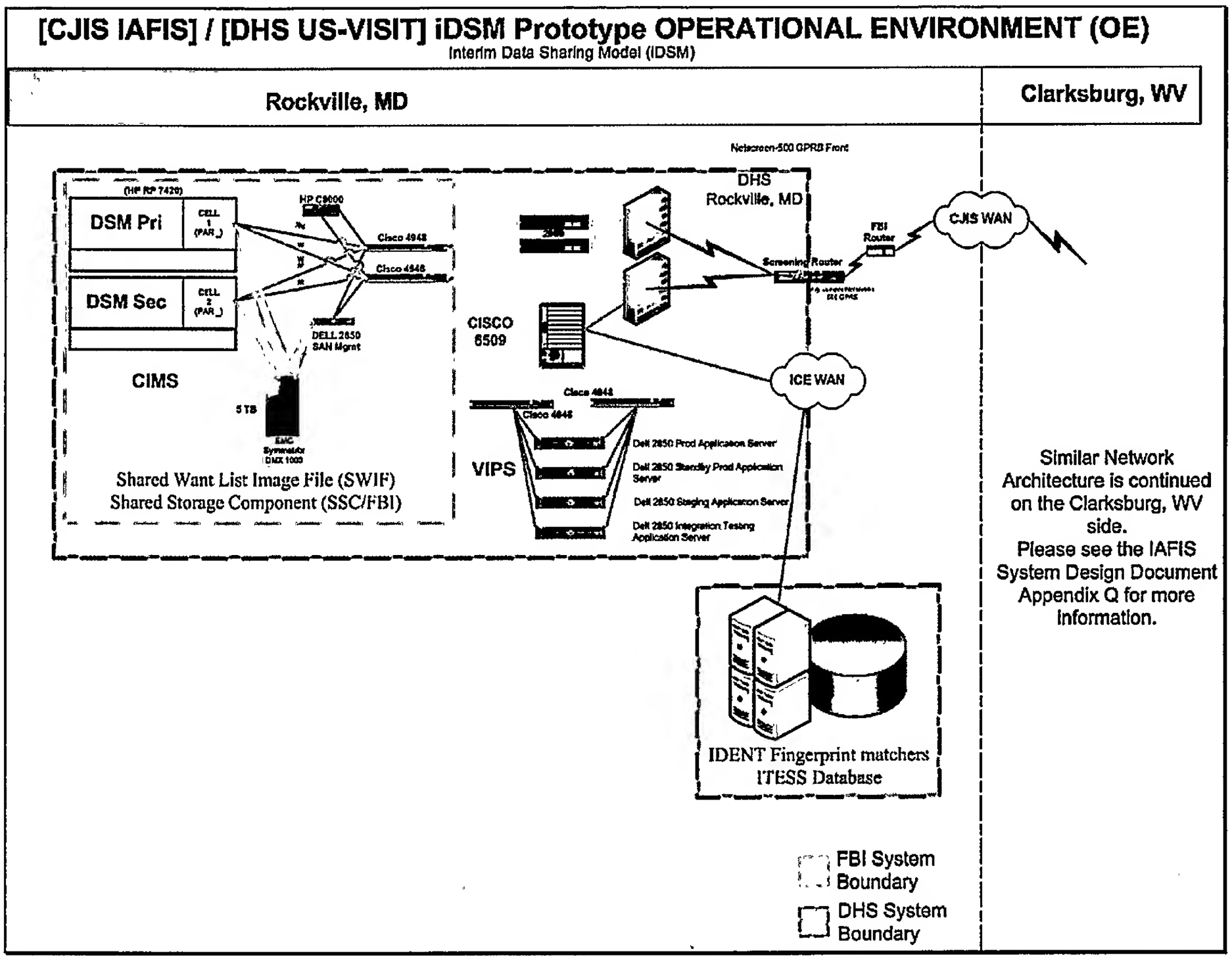
IAFIS external communications interfaces are comprised of four external connections via the CJIS Wide Area Network (WAN). EFCON/FBI provides an interface to the CJIS Wide Area Network (WAN). NCIC and Nlets communicate directly with III/FBI. Each of these interfaces includes different complements of communication protocols. The IAFIS/FBI Front End systems will interface as a node to the WAN network management service.

The CJIS WAN Service Delivery Point(s) (SDPs) will be the external demarcation points at the JEH, Woodies, G Street, and Gallery Row facilities located in Washington, D.C. Other SDPs will be external demarcation points at Quantico, VA; Dover, DE; Aiken, SC; Fairmont, WV; and Clarksburg, WV facilities. The FBI will determine the interface points at all of these locations.

The Rockville, MD, location is a Department of Justice data center. This location houses the CIMS component of the iDSM segment similar to how the VIMS component of iDSM/DHS is housed in the CJIS/FBI data center. The iDSM network topology will allow each agency to be in a remote data center, but maintain network freedom within its own enclave (

Figure 4.1.1-1 shows an example of this). The firewalls configured in each location will limit connectivity in and out of the enclaves, but within the enclave, the rules will allow traffic to flow freely. The firewall rules will be different in each location due to the different methods of message transport. The configuration of the firewalls will allow web service traffic to communicate between the enclaves within a single data center. Each data center will control the firewalls and network devices that will physically reside in the buildings.

Figure 4.1.1-1 Example of a iDSM Network Enclave



Communication entering Rockville from Clarksburg will go through a screening router and then into the firewall. The firewall monitors all traffic coming into and out of the systems and makes a determination if the traffic is allowed to enter. The reverse will be true for Clarksburg. Communication entering Clarksburg from Rockville will go through a screening router and then into the firewall. Communication from VIMS to CIPS will return through the same firewall. Communication from CIPS to IAFIS will not go through the same firewall.

4.1.1.1 Physical Layer Interface

The EFCON/FBI Front End will interface with the Single Attached Station (SAS) Firewall(s) through the EFCON/FBI Cisco Catalyst 6513 switch. The demark for EFCON/FBI Front End will be the Single Attachment Source (SAS) Gigabit Ethernet/Category 5e (Cat5e) cable interface on the Firewall(s). The CAT5e interface will support up to 1 Gigabit per second (Gbps) of traffic to and from the CJIS WAN. The attached devices and cabling will meet Institute of Electrical and Electronic Engineers (IEEE) standard 802.ab (1000Base-T). The cable installation will support Federal Information Processing Standard (FIPS) PUB 174, also known as the Federal Building Telecommunication Wiring Standard and Federal Information Processing Standard (FIPS) PUB 175, also known as Federal Building Standard for Telecommunications Pathways and Spaces.

4.1.1.2 Data Link Layer Interface

The IAFIS/FBI Data Link interface between the EFCON/FBI servers and the CJIS WAN SAS Firewall(s) will be Gigbit Ethernet in accordance with the IEEE standard 802.3ab (1000Base-T). The devices will also support IEEE standards 802.1D "Media Access Control Bridges" or Spanning Tree Protocol as needed and IEEE standard 802.1Q "Virtual Local Area Networks" as needed.

4.1.1.3 Network Layer Interface

The network layer interface between the ITN/FBI Front End system and CJIS WAN will be based on Request For Comment (RFC) 791, "Internet Protocol" (IP). Additional parameters for the Internet Protocol can be found in RFC 1349 "Types of Service in the Internet Protocol Suite" and 2474 "Definition of the Differentiation Service Field (DS Field) in the IPv4 and IPv6 headers" where some portions of RFCs 1349 and 2474 have made RFC 791 obsolete. Further, this interface will support appropriate applications in RFC 894 "Standard for Transmission of IP Datagrams Over Ethernet Networks," and RFC 792 "Internet Control Message Protocol" (ICMP) in addition to portions of RFC 792 made obsolete by RFC 950 "Internet Standard Subnetting Procedure." Also Network Layer Interfaces may need to support RFC 1883 "Internet Protocol, version 6, IPv6 Specification" and those portions of RFC 2460 "Internet Protocol, version 6, IPv6 Specification" that make RFC 1883 obsolete. Additional support for RFC 4293 "Management Information Base for the Internet Protocol' will be used as needed. Support may be needed for RFC 1042 "Standard for Transmission of IP Datagrams over IEEE 802 Networks."

4.1.1.4 Transport Layer Interface

The transport layer interface between the EFCON/FBI Front End system and CJIS WAN components will be in accordance with the RFC 793 "Transmission Control Protocol" (TCP) and portions of RFC 3168 "The addition of Explicit Congestion Notification (ECN) to IP" which

portions make RFC 793 obsolete. In addition to supporting RFC 793, RFC 768 "User Datagram Protocol" will also be supported as needed. Also, support for the standards RFC 1700 "Assigned Numbers (port/sockets)" and those portions of RFC 1700 made obsolete by RFC 3232 "Assigned Numbers: RFC 1700 is replaced by an Online Database" and the Internet Assigned Numbers Authority (IANA; www.iana.org) organization will be implemented.

4.1.1.5 Application Layer Interface

The application layer interface between the IAFIS FE and CJIS WAN will support RFC 821 "Simple Mail Transfer Protocol" (SMTP) and those portions of RFC 821 made obsolete by RFC 2821 "Simple Mail Transfer Protocol." In addition, the application Layer interface will support RFCs 1521 and 1522, Parts One and Two of Multipurpose Internet Mail Extensions (MIME) and portions of RFC 1521 and RFC 1522 made obsolete by RFC 2045 "Multipurpose Internet Mail Extension (MIME) Part One: Format of Internet Message Bodies," RFC 2046 "Multipurpose Internet Mail Extension (MIME) Part Two: Media Types," RFC2047 "Multipurpose Internet Mail Extension (MIME) Part Three: Message Header Extension for Non-ASCII Text," RFC 2048 "Multipurpose Internet Mail Extension (MIME) Part Four: Registration Procedures," RFC 4288 "Multipurpose Internet Mail Extension (MIME) Media Types and Registration Procedures, RFC 2049 "Multipurpose Internet Mail Extension (MIME) Part Five: Conformance Criteria and Examples," RFC 2184 "MIME parameter values and Encoded Word Extension, Character Sets, Languages, and Continuations," RFC 2231 "MIME parameter values and Encoded Word Extension, Character Sets, Languages, and Continuations," RFC 2646 "Multipurpose Internet Mail Extension (MIME) Text/Plain Format Parameter," RFC 3676 "Multipurpose Internet Mail Extension (MIME)) Text/Plain Format Parameter and DelSp," and RFC 3798 "Multipurpose Internet Mail Extension (MIME) Message Disposition Notification." As an option, the interface will support ITU-T X.400-1988 Application Program Interface (API) Draft 3.

4.1.2 IAFIS FE—NCIC Interface

The IAFIS FE shall have the capability of interfacing to the NCIC Processor and states via NCIC.

4.1.2.1 Physical Layer Interface

The CJIS WAN Front End (or gateway routers) will be capable of supporting RS-232-C/V.24 and V.35 interfaces for various NCIC links as required. The cabling for the connectivity will also support FIPS PUB 174 and FIPS PUB 175. The demarcation point for IAFIS Front End will be the Single Attachment Source (SAS) Gigabit Ethernet/Category 5e (Cat5e) cable interface on the NCIC Firewall(s). The CAT5e interface will support up to 1 Gigabit per second (Gbps) of traffic to and from the CJIS WAN. The attached devices and cabling will meet IEEE standard 802.ab (1000Base-T). The cable installation will support Federal Information Processing Standard (FIPS) PUB 174, also known as the Federal Building Telecommunication Wiring Standard and

Federal Information Processing Standard (FIPS) PUB 175, also known as Federal Building Standard for Telecommunications Pathways and Spaces.

4.1.2.2 Data Link Layer Interface

The Data link layer interface between the CJIS WAN Front End and NCIC Front End system and devices will support IEEE standards 802.1D "Media Access Control Bridges" and 802.1Q "Virtual Local Area Networks." Devices will be Gigbit Ethernet in accordance with the IEEE standard 802.3ab (1000Base-T).

4.1.2.3 Network Layer Interface

The network layer interface between the NCIC Front End system and CJIS WAN will be based on Request For Comment (RFC) 791, "Internet Protocol" (IP). Additional parameters for the Internet Protocol can be found in RFC 1349 "Types of Service in the Internet Protocol Suite" and 2474 "Definition of the Differentiation Service Field (DS Field) in the IPv4 and IPv6 headers" where some portions of RFCs 1349 and 2474 have made RFC 791 obsolete. Further, this interface will support appropriate applications in RFC 894 "Standard for Transmission of IP Datagrams Over Ethernet Networks" and RFC 792 "Internet Control Message Protocol" (ICMP) in addition to portions of RFC 792 made obsolete by RFC 950 "Internet Standard Subnetting Procedure." Also Network Layer Interfaces may need to support, as needed, RFC 1883 "Internet Protocol, version 6, IPv6 Specification" and those portions of RFC 2460 "Internet Protocol, version 6, IPv6 Specification" that make RFC 1883 obsolete. Additional support for RFC 4293 "Management Information Base for the Internet Protocol" will be used as needed. Support may be needed for RFC 1042 "Standard for Transmission of IP Datagrams over IEEE 802 Networks."

4.1.2.4 Transport Layer Interface

The transport layer interface between the IAFIS Front End and NCIC components will be in accordance with the RFC 793 "Transmission Control Protocol" (TCP) and portions of RFC 3168 "The addition of Explicit Congestion Notification (ECN) to IP" which portions make RFC 793 obsolete. In addition to supporting RFC 793, RFC 768 "User Datagram Protocol" will also be supported as needed. Also, support for the standards RFC 1700 "Assigned Numbers (port/sockets)" and those portions of RFC 1700 made obsolete by RFC 3232 "Assigned Numbers: RFC 1700 is replaced by an Online Database" and the Internet Assigned Numbers Authority (IANA; www.iana.org) organization will be implemented.

4.1.2.5 Application Layer Interface

The application layer interface will support the NCIC messages as defined in Appendix A, IAFIS MDD.

4.1.3 IAFIS FE—Nlets Interface

The CJIS Systems Agencies (CSAs) will use the Transmission Control Protocol/Internet Protocol (TCP/IP) in accordance with IBM GA27-3004.

4.1.3.1 Physical Layer Interface

The CJIS WAN Front End (or gateway routers) will be capable of supporting RS-232-C/V.24 and V.35 interfaces for various NCIC links as required. The cabling for the connectivity will also support FIPS PUB 174 and FIPS PUB 175. The demarcation point for IAFIS Front End will be the Single Attachment Source (SAS) Gigabit Ethernet/Category 5e (Cat5e) cable interface on the NCIC Firewall(s). The CAT5e interface will support up to 1 Gigabit per second (Gbps) of traffic to and from the CJIS WAN. The attached devices and cabling will meet IEEE standard 802.ab (1000Base-T). The cable installation will support Federal Information Processing Standard (FIPS) PUB 174, also known as the Federal Building Telecommunication Wiring Standard and Federal Information Processing Standard (FIPS) PUB 175, also known as Federal Building Standard for Telecommunications Pathways and Spaces.

4.1.3.2 Data Link Layer Interface

The data link layer interfaces between the IAFIS FE and Nlets will support TCP/IP in accordance with IBM GA27-3004. The Data link layer interface between the IAFIS Front End and Nlets Front End system and devices will support IEEE standards 802.1D "Media Access Control Bridges" and 802.1Q "Virtual Local Area Networks." Devices will be Gigbit Ethernet in accordance with the IEEE standard 802.3ab (1000Base-T).

4.1.3.3 Network Layer Interface

The network layer interface between the IAFIS Front End system and Nlets will be based on Request For Comment (RFC) 791, "Internet Protocol" (IP). Additional parameters for the Internet Protocol can be found in RFC 1349 "Types of Service in the Internet Protocol Suite" and 2474 "Definition of the Differentiation Service Field (DS Field) in the IPv4 and IPv6 headers" where some portions of RFCs 1349 and 2474 have made RFC 791 obsolete. Further, this interface will support appropriate applications in RFC 894 "Standard for Transmission of IP Datagrams Over Ethernet Networks," and RFC 792 "Internet Control Message Protocol" (ICMP) in addition to portions of RFC 792 rendered obsolete by RFC 950 "Internet Standard Subnetting Procedure." Also Network Layer Interfaces may need to support RFC 1883 "Internet Protocol, version 6, IPv6 Specification" and those portions of RFC 2460 "Internet Protocol, version 6, IPv6 Specification" that make RFC 1883 obsolete. Additional support for RFC 4293 "Management Information Base for the Internet Protocol' will be used as needed. Support may be needed for RFC 1042 "Standard for Transmission of IP Datagrams over IEEE 802. Networks."

4.1.3.4 Transport Layer Interface

The IAFIS Front End and Nlets Front End will be in accordance with the RFC 793 "Transmission Control Protocol" (TCP) and portions of RFC 3168 "The addition of Explicit Congestion Notification (ECN) to IP" which portions render RFC 793 obsolete. In addition to supporting RFC 793, RFC 768 "User Datagram Protocol" will also be supported as needed. Also, support for the standards RFC 1700 "Assigned Numbers (port/sockets)" and those portions of RFC 1700 made obsolete by RFC 3232 "Assigned Numbers: RFC 1700 is replaced by an Online Database" and the Internet Assigned Numbers Authority (IANA; www.iana.org) organization will be implemented.

4.1.3.5 Application Layer Interface

The application layer interface between the IAFIS/FBI FE system and Nlets will support the messages as listed in Appendix K and defined in Appendix A, IAFIS MDD.

4.2 IAFIS Internal Communication Interfaces

Internal communications interfaces on the IAFIS/FBI FE will be provided by ITN/FBI. Major segments such as the III/FBI, AFIS/FBI, iDSM/FBI and ITN/FBI, or other systems will interface with the ITN/FBI Backbone Communication Element (BCE) and with internal communications interfaces on the ITN/FBI network being provided by the ITN/FBI.

4.2.1 Physical Layer Interface

The FBI will define the Wide Area Network (WAN) Virtual Private Network (VPN) Service Delivery Point(s) (SDPs) for the JEH, Woodies, G Street, and Gallery Row facilities located in Washington, D.C. Other SDPs will be at Quantico, VA; Dover, DE; Aiken, SC; Fairmont, WV; and Clarksburg, WV facilities. The FBI will determine the interface points at all of these locations.

4.2.2 Physical Layer Interface

The physical layer connectivity between the ITN/FBI Backbone and AFIS/FBI, III/FBI, and iDSM/FBI will be Gigabit Ethernet in accordance with IEEE 802.3ab (1000Base-T). The attached devices and cabling will meet IEEE standard 802.ab (1000Base-T). The cable installation will support Federal Information Processing Standard (FIPS) PUB 174, also known as the Federal Building Telecommunication Wiring Standard and Federal Information Processing Standard

(FIPS) PUB 175, also known as Federal Building Standard for Telecommunications Pathways and Spaces.

4.2.3 Data Link Layer Interface

The data link layer interface between the ITN/FBI Backbone and AFIS/FBI, III/FBI, and iDSM/FBI will be GigE in accordance with IEEE 802.3ab (1000Base-T). The devices will also support IEEE standards 802.1D "Media Access Control Bridges" or Spanning Tree Protocol as needed and IEEE standard 802.1Q "Virtual Local Area Networks" as needed.

4.2.4 Network Layer Interface

The network layer interface between the ITN/FBI Backbone Element and AFIS/FBI, III/FBI, and iDSM/FBI will be in accordance with Request For Comment (RFC) 791, "Internet Protocol" (IP). Additional parameters for the Internet Protocol can be found in RFC 1349 "Types of Service in the Internet Protocol Suite" and 2474 "Definition of the Differentiation Service Field (DS Field) in the IPv4 and IPv6 headers" where some portions of RFCs 1349 and 2474 have made RFC 791 obsolete. Further, this interface will support appropriate applications in RFC 894 "Standard for Transmission of IP Datagrams Over Ethernet Networks" and RFC 792 "Internet Control Message Protocol" (ICMP) in addition to portions of RFC 792 made obsolete by RFC 950 "Internet Standard Subnetting Procedure." Also Network Layer Interfaces may need to support, as needed, RFC 1883 "Internet Protocol, version 6, IPv6 Specification" and those portions of RFC 2460 "Internet Protocol, version 6, IPv6 Specification" that make RFC 1883 obsolete. Additional support for RFC 4293 "Management Information Base for the Internet Protocol' will be used as needed. Support may be needed for RFC 1042 "Standard for Transmission of IP Datagrams over IEEE 802. Networks."

4.2.5 Transport Layer Interface

The transport layer interface between the ITN/FBI BCE and AFIS/FBI, III/FBI, and iDSM/FBI will be in accordance with the RFC 793 "Transmission Control Protocol" (TCP) and portions of RFC 3168 "The addition of Explicit Congestion Notification (ECN) to IP" which portions make RFC 793 obsolete. In addition to supporting RFC 793, RFC 768 "User Datagram Protocol" will also be supported as needed. Also, support for the standards RFC 1700 "Assigned Numbers (port/sockets)" and those portions of RFC 1700 made obsolete by RFC 3232 "Assigned Numbers: RFC 1700 is replaced by an Online Database" and the Internet Assigned Numbers Authority (IANA; www.iana.org) organization will be implemented.

4.2.6 Application Layer Interface

The application layer interface will consist of the on-line transaction processing software complement called Tuxedo. Image file transfers between ITN/FBI and AFIS/FBI will be via NFS as described by internet RFC 1813 "Networked File System version 3 (NFS) Protocol Specification" and internet RFC 1305 "Network Time Protocol version 3 Specification, Implementation, and Analysis." Also, both the ITN/FBI to III/FBI and ITN/FBI to AFIS/FBI will include Network Time Protocol and SQL*Net as defined in ANSI X3.135-1992—Database Language SQL. Messages destined for users via NCIC circuits will be blocked and segmented by III/FBI based on information contained in the Multiblock HeaderCode (MHC) field.

Web-based applications and mail are provided over the CJIS WAN for the different systems. These services are HTTP (80), HTTPS (443), and SMTP (25). The iDSM/FBI connectivity to the ITN/FBI, III/FBI, and AFIS/FBI will include NTP and SQL*Net as defined in ANSI X3.135-1992-Database Language SQL. Messages destined for users via NCIC or NCIC circuits will be blocked and segmented by III/FBI based on information contained in the Multiblock Header Code (MHC) field.

4.2.7 System Administration

IAFIS is a distributed processing system with some system administration (SA) functions common to two or more segments. To provide standardized system administration, SA functions common to two or more of the IAFIS segments are defined in the paragraphs below.

4.3 Functional Message Header

All messages exchanged between IAFIS segments shall contain a header, as defined in the Message Definition Database (MDD), Data Set "IAFISHDR."

4.4 Clock Synchronization Message

The ITN/FBI clock will be synchronized with an external standard reference time, such as the Coordinated Universal Time (UTC), with accuracy better than 0.05 seconds. The other IAFIS segments/elements are to sync with the ITN/FBI clock at intervals sufficient to ensure that this synchronization is maintained within 0.05 second margin in accordance with the appropriate applications in RFC 1305, Network Time Protocol (NTP).

4.5 Acknowledgment Messages

Messages and transactions between IAFIS segments do not require Acknowledgments (ACKs) or Not Acknowledged (NAKs) other than those provided by the ITN/FBI BCE as a matter of normal communications processing [(Data Link layer of the Open System Interconnection/Reference Model (OSI/RM)]. The iDSM has a PERL program that polls a specific directory and sends SMTP messages back to IWS. This is used to send ACK messages for Insert/Update and Demote/Remove commands. It sends confirmation messages from the Wlist_RSP_WS_FD web service. Messages of a time- or priority-critical nature which are deemed necessary to provide special ACK/NAK service are defined in the MDD.

4.6 System Status Messages

Each segment is responsible for notifying other segments and external users of scheduled outages.

4.7 Billing Information

Certain IAFIS customers must pay for IAFIS services. IAFIS will administer an accounting and billing system for those customers. Billing will be accomplished through IDWH/FBI User Fee Billing Sub-element (UFBS). The data necessary for billable transactions are documented in the MDD.

4.8 Operating Environments

IAFIS will provide multiple environments to make its operation and maintenance easier. Service providers, operators, developers, external users, and testers will be able to access special environments for training, development, and testing. IAFIS will be able to provide these services simultaneously while protecting the integrity of each environment. Nominally, the workloads of these support environments and the resources allocated to them will be approximately 10% of those for the operational environment. The boundaries between the training, development, testing, and operational environments and the amount of resources allocated to each will be under IAFIS system administrator control and will be adjustable to meet dynamic requirements. As noted in paragraph 1.5, segment developers are required to provide these operating environments within their segments.

4.8.1 Test Support Environment

IAFIS will provide test support environments that provide a means to integrate and verify hardware and software capabilities and to assess operational effectiveness and suitability. The test support environments will support testing of new or upgraded hardware, testing of inter-segment and intra-IAFIS interfaces, testing of software upgrades in any segment, and end-to-end testing of IAFIS functions. The test support environments will protect the operational IAFIS from corruption by test processes. IAFIS will identify all test-related interactions between IAFIS and external systems and between segments as test transactions, and each segment will restrict test-related processing to the test support environment.

4.8.1.1 External User Testing

The test support environment will support external user submission of test transactions to IAFIS. The external user may submit test transactions to ensure that his equipment is properly interconnected and that the transaction is correctly formatted. The test support environment response to external user tests will consist of test data in a format that parallels responses of the operational system. The test support environment will support external user testing using the same telecommunications equipment as the operational system. External users must coordinate access to the IAFIS test support environment with the System Administrator.

4.8.1.2 Support for IAFIS-level, End-to-End Testing

The test support environment will provide the capability to test the integration and interoperation of the segments, to identify defects, and to test IAFIS functionality, throughput, and performance. The test support environment will support pre-implementation testing of emergency fixes before they are promoted to the operational system. The test support environment will support certification and acceptance testing prior to the release of IAFIS updates and modifications to production operations.

4.9 Error Processing and Exception Handling

Between the time a segment receives a request and the time the segment provides a response to that request, a processing error may occur. The cause of the error may be one of several possibilities including a formatting error in the request message, a system outage in the responding segment, or a logical database error such as trying to modify a record that does not exist. In any case, it is incumbent on the responding segment (or accepting segment in the case of the NR protocol) to indicate the nature of the error to the requesting segment so that the cause of the error can be investigated and corrected.

4.9.1 Error Notification Message

The A1802 message will be used to notify a requesting segment when an error has been detected while processing its request. It is defined in the Message Definition Database (MDD). The values to be used in set ERRMSGSET are defined in the Error Codes table in the MDD. When the error is to be reported to a service provider or external user, the Error Description in the Error Codes table suggests how the element values may be used to form descriptive text. The following paragraphs describe the contents of the messages and how the messages are used.

4.9.2 Number of Occurrences

A single error notification message may indicate up to ten error conditions belonging to the same error type (see Table 3-1). A field in the Tuxedo physical view tells the segment receiving the Error Notification messages how many error conditions are included in the message.

4.9.3 Error Identifier (MSGCOD)

Each error condition is identified by an error identifier code using the MSGCOD field. The identifier is composed of 5 characters. The first character indicates the type of error as shown in Table 3-1. The remaining 4 characters identify the specific condition within that type. Only one type of error is reported in one A1802 message. Error identifiers are defined in the MDD.

4.9.4 Error Inserts (MSGINSCNT and MSGINS)

The MSGINSCNT and MSGINS fields provide specific information related to the error identifier. For example, if the error condition is that a message does not include a value for a mandatory field, an error insert would provide the name of the field that was not included. That allows the use of generic error identifiers (e.g., "Missing Mandatory Field") rather than specific error identifiers (e.g., "Missing Name Field," "Missing Race Field," etc.). The MSGINSCNT indicates the number of error inserts related to the error identifier. The MSGINS fields provide the error inserts. The number of inserts used and the type of information provided by the error inserts is dependent on the error identifier. The Error Codes table in the MDD defines the number of inserts and data provided for each error identifier.

4.9.5 Use of the A1802 Error Message with Intersegment Protocols

4.9.5.1 Immediate Response (IR) Protocol

An A1802 message can be the response to a request sent using the IR protocol. In this case, the A1802 will be the only response to the request as indicated in Figure 4.9.5.1-1.

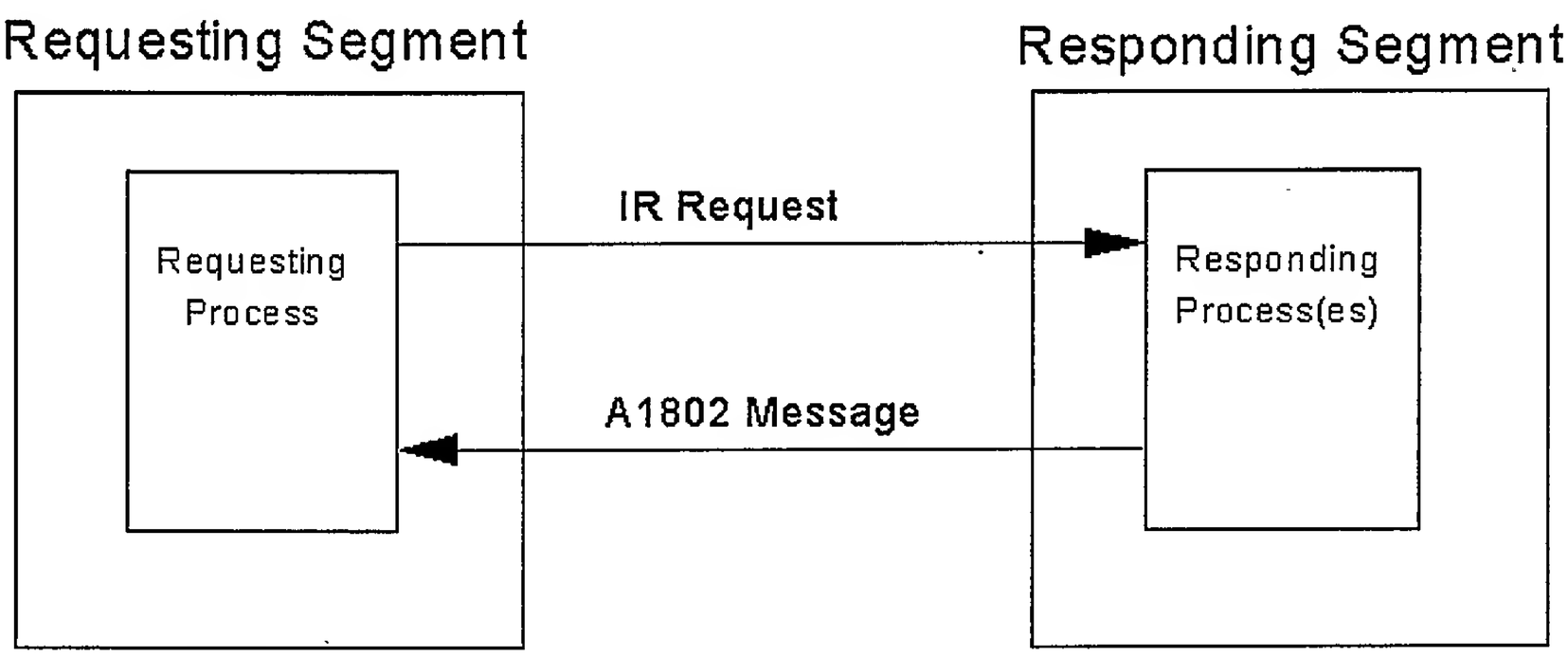


Figure 4.9.5.1-1 Use of A1802 With IR Protocol

If the A1802 contains any error other than a Warning-type, it will indicate that the request failed and that the requesting segment should take action as indicated in Table 3-1.

Table 4-1 Intersegment Message Error Types

Error Type	Description
H Header	An error is detected in any of the IAFIS header elements. It could be a formatting error in an element or an error due to a combination of multiple elements. It could also be that the message is not appropriate for the service initiated. This type of error is unrelated to the contents of the message. Upon receipt of this type of error message, a segment should record the error message and the message that caused the error and then notify a segment administrator. The message should not be retransmitted.

Error Type	Description
E Element	An error is detected in one or more of the message elements (not including the IAFIS header). This error type is also used in reporting incoming EBTS message errors. This type of error is returned when an element value is of the wrong type (alpha/numeric) or outside of the allowable range such as an unallowable hair color. Upon receipt of this type of error in an A1802 message, a segment should record the error message and the message that caused the error and then notify a segment administrator. The message should not be retransmitted.
S Segment Status	An error occurs that prohibits the segment from completing the processing of a request. The error is most likely caused by a software error. Upon receipt of this type of error message, a segment should record the error message and the message that caused the error and then notify a segment administrator. The message should not be retransmitted.
R Retry	An error occurs that is correctable. It could be that the service that is needed is temporarily unavailable or that the database is closed. Upon receipt of this type of error message, a segment should wait for a short period (two minutes) and resend the original message. Two retries may be attempted before giving up and notifying a segment administrator.
L Logic	An error occurs because the processing rules prohibit the requested operation on the specified data. For example, a transaction may require that a subject's features be deleted, but they do not exist. A segment must refer this type of error to a service provider for a determination of the cause of the error.
A Authorization	An error is detected when an operation is requested but the requestor is not authorized. A segment must refer this type of error to a service provider and allow the transaction to be re-routed to someone who is authorized.
W Warning	This error type is used whenever the transaction is able to complete, but the service wishes to provide some information back to the requester. For example, III may provide routing information following a successful file maintenance operation. A segment must be prepared to act on these messages as appropriate, such as providing information to a service provider or changing the workflow based on the warning.

An A1802 message can be received by a requesting segment due to a KR request in two ways. The first may occur if the responding segment finds an error in the request before acknowledging the request such as with a header error. In this case, the A1802 is returned as an immediate response to the KR request and no further processing is performed by the responding segment (see Figure 4.9.5.1-2).

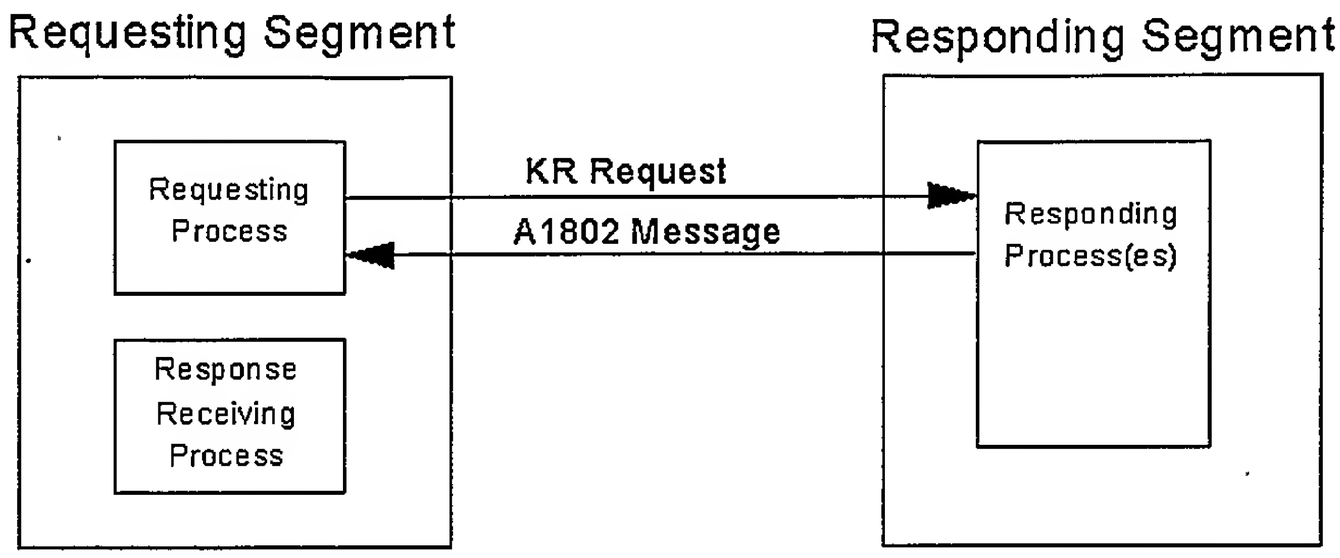


Figure 4.9.5.1-2 Use of A1802 With KR Protocol – Immediate Error

The second case may occur if the responding segment detects an error after positively acknowledging receipt of the request such as when a logic error is determined. In this case, the responding segment sends the A1802 message as the message in the response part of the KR protocol (see Figure 4.9.5.1-3).

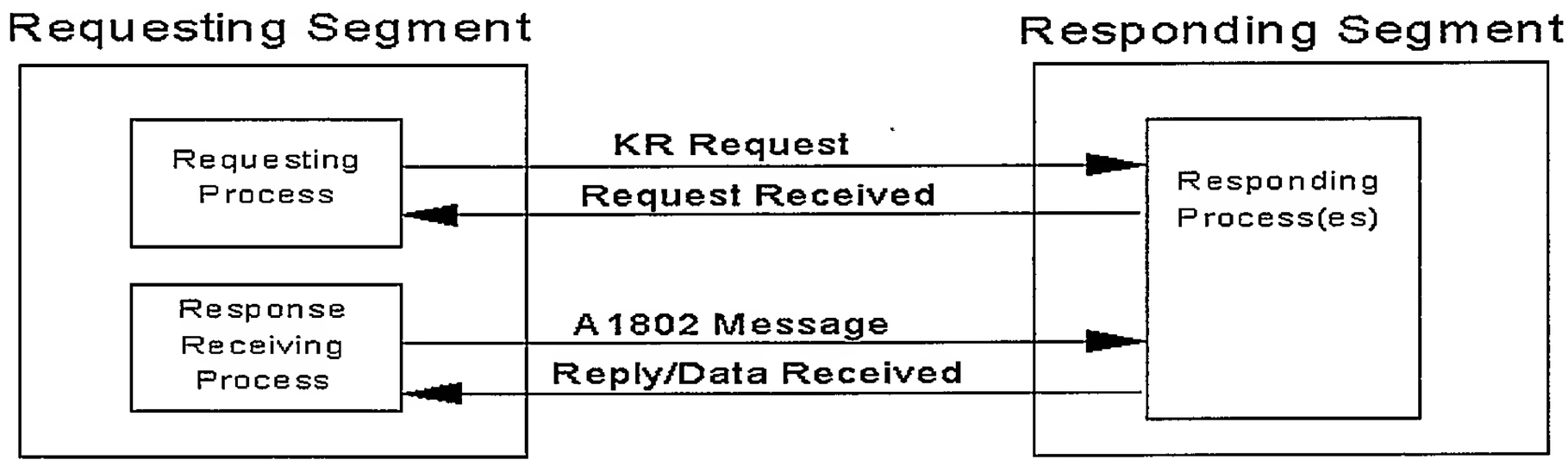


Figure 4.9.5.1-3 Use of A1802 With KR Protocol – Response Error

An A1802 message can also be received by the responding segment due to a KR response that it sends. When the requesting segment receives the response and is not able to accept it due to an error, the requesting segment will return an A1802 to the responding segment instead of sending a positive acknowledgment (see Figure 4.9.5.1-4).

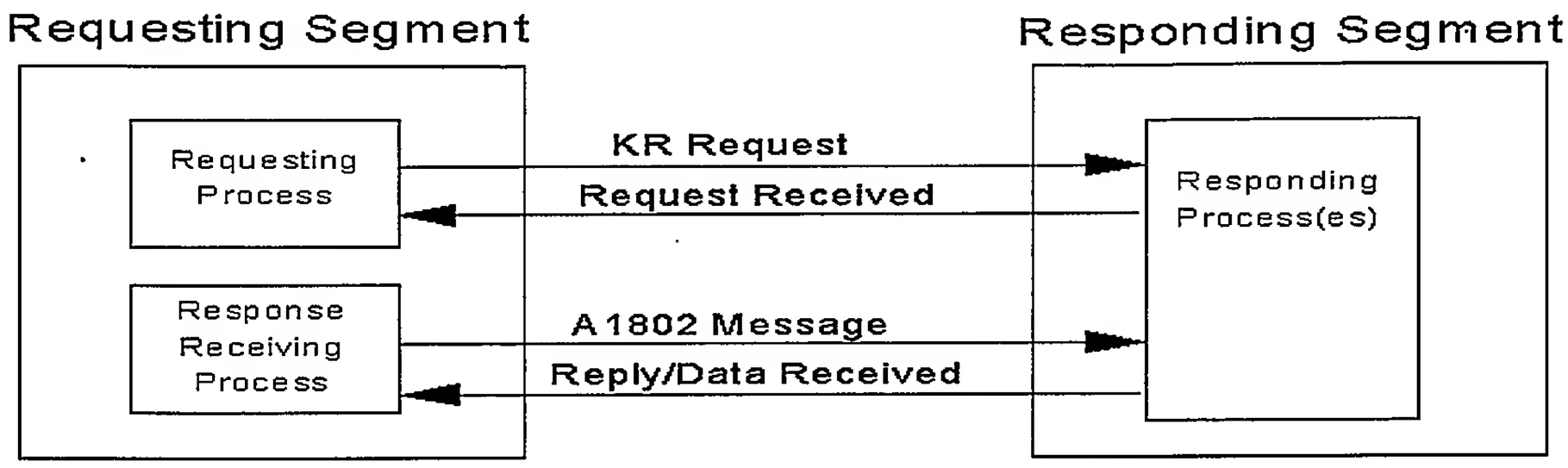


Figure 4.9.5.1-4 Use of A1802 With KR Protocol – Normal Response

4.9.5.2 No Response (NR) Protocol

After sending a request using the NR protocol, an A1802 message can be received by a requesting segment instead of a positive acknowledgment as shown in Figure 4.9.5.2-1.

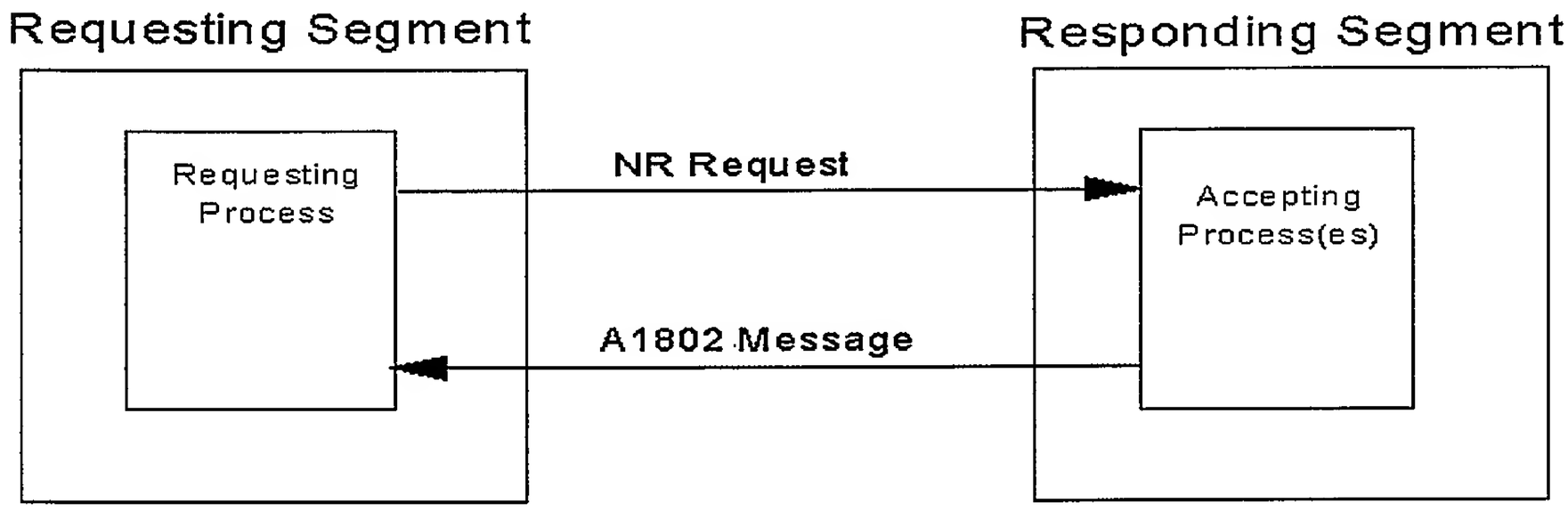


Figure 4.9.5.2-1 Use of A1802 With NR Protocol

4.9.5.3 Unsolicited Error Notification

If the requesting segment detects an error in the response *after* it has positively acknowledged the response, it may send an unsolicited A1802 error message to the responding segment. The purpose of this message is to alert the responding segment to the fact that its response was found to be in error or that the requesting segment was unable to match the response up with its re-

quest. This capability may also be used by segments to notify one another about segment outages.

4.9.6 Examples of Error Messages

Example 1—Header Error

A segment receives a message, but the STOT value is determined to be "AAAA." The segment returns an A1802 message containing the following fields:

- NOO = 1
- MSGCOD(1) = H0003
- MSGINSCNT(1) = 2
- MSGINS (1,1) = "STOT"
- MSGINS (1,2) = "AAAA"
- MSGINS (1,3) = NULL

Example 2—Element Errors

A segment receives a message, but the SEX field contains a disallowed value "B" and the RAC field, which is mandatory for this message, is missing. The segment returns an A1802 message containing the following fields:

- NOO = 2
- MSGCOD(1) = E0003
- MSGINSCNT(1) = 2
- MSGINS(1,1) = "SEX"
- MSGINS(1,2) = "B"
- MSGINS(1,3) = NULL
- MSGCOD(2) = E0001
- MSGINSCNT(2) = 1
- MSGINS(2,1) = "RAC"
- MSGINS(2,2) = NULL
- MSGINS(2,3) = NULL

The order of the error codes is not important.

Example 3—Logic Error

A segment receives a message that requests retrieval of fingerprint images for FBI number 123456AA. The segment attempts to retrieve that subject's fingerprint images and discovers that

no images exist for that FBI number. The segment returns an A1802 message containing the following fields:

- NOO = 1
- MSGCOD(1) = L0004
- MSGINSCNT(1) = 1
- MSGINS(1,1) = "123456AA"
- MSGINS(1,2) = NULL
- MSGINS(1,3) = NULL

5 REQUIREMENTS TRACEABILITY

5.1 SRD Requirements Traceability

All requirements traceability information is now being kept in the Requisite Pro tool.

APPENDIX A IAFIS MESSAGE DEFINITIONS

A.1 CJIS Messages

The exchange of information is an essential activity among IAFIS and other CJIS components. The existing CJIS systems were developed independently, resulting in some conflicting data elements, data codes, and message structures. A fundamental goal is for the evolutionary resolution of conflicts and coordinated development among the CJIS systems. To be certain that the information exchanged is current, accurate, concise, and understandable, an IAFIS MDD standard has been created and is installed in this ICD as Appendix A. The MDD uses a controlled vocabulary (including abbreviations and codes) for which unambiguous meanings are defined.

The MDD provides configuration management control of the messages specified in this appendix. This includes the IAFIS-bound messages from NCIC and Nlets and from those entering via the CJIS WAN. The MDD provides:

- a basic architectural structure
- semantics (artificial language system to define vocabulary)
- syntax (rules governing structure and arrangement of message components)

The MDD architectural structure for message definition has four subdivisions: messages, reports format, sets, and elements. These can be equated to the FBI message definition terminology as messages, response reports format, data compounds, and data elements (or messages, object definitions, and primitives for NCIC).

A.2 Document Description

This appendix defines the messages exchanged between functional entities within and outside IAFIS. Physical connectivity is defined in Section 4 of the ICD. Details of physical path routing related to internal or external stimulus message (e.g., internally-generated Subject Search, externally-generated Ten-Print Submission) are found in Appendix B. The following prefixes are used to identify the MDD Message location in the CJIS System:

A:	Messages internal to IAFIS
E:	EBTS Messages to/from the EFCON/FBI FE
N:	Messages to/from NCIC
L:	Messages to/from Nlets

The following numbering conventions have been used to assign unique identification numbers to each IAFIS message:

- Submission and Response Data Messages are defined in the A1000–A1999 range,
- File Maintenance and III Administrative Messages are defined in the A3000–A3999 range,
- Performance Monitoring, System Administration, and User Fee Billing Messages are defined in the A5000–A5999 range, and
- Miscellaneous Messages are defined in the A9000–A9999 range.

Note that the message numbers do not always run consecutively.

The structural notation used in the IAFIS MDD is used to describe relationships that exist among the message components. The structural notation used is a modified form of Backus-Naur Notation. The following symbols are used in this notation:

=	means *is equivalent to*
+	means *and*
|	means *or*
[|]	means *must choose one of the components separated within the brackets*
{}	means *iterations of the component enclosed, where lower limit is placed to the left of the opening bracket and upper limit is placed to the right of closing bracket*
()	means *the enclosed component is optional*
""	means *component enclosed within quotes is a literal value*
◇	means *enclosed component modifies or qualifies component to its left*

A.3 Assumptions and Constraints

Although the MDD documents message structure, it does not specify communication protocols (e.g., "eot"- end of transmission), field separator characters (e.g., —repeat field separator), or other message/field parsing designators. There are two notable exceptions to this general rule; these details will be provided in support of the existing legacy messages and the EBTS transactions fielded by IAFIS via the CJIS WAN. Use of these designators is left to the respective vendors to implement in accordance with FBI standards.

Where appropriate, message names are consistent with the NCIC naming convention.

Note

All of the CJIS Message Definitions in Appendix A are reproduced electronically from the Message Definition Database (MDD) housed in an on-line database. They are available only in hardcopy format from IAFIS CM, or may be produced using the MDD tool, also available from CM.

APPENDIX B SEQUENCING AND NOTES

B.1 Document Description

This appendix defines the physical routing of all messages exchanged (i.e. data flow) between functional entities internally and externally to IAFIS. Physical connectivity is defined in Section 4 of the ICD.

This appendix is organized into five sections, the first, Section 20, being an Introduction. Sections 21 through 23 respectively, define:

- Mission-Critical Message Data Flow,
- Maintenance and Administration Message Data Flow, and
- Operations and User Fee Billing Data Flow.

Notes on Diagram

The data flow diagrams show the flow of data messages between IAFIS Segments and selected entities external to IAFIS; refer to the appropriate requirements document for details of the processing logic within the segments. Processing internal to a segment is not depicted herein (e.g., the retrieval of images from ISRE is not explicitly shown, because that activity is internal to ITN/FBI).

The IAFIS Data Flow Diagrams in this appendix were developed in accordance with the following paradigm:

- Data Flow Diagrams whose original stimulus messages are transmitted to the FBI by electronic means (i.e., NCIC Telecommunications, CJIS WAN, or Nlets) are listed as "External" to IAFIS.

  Data Flow Diagrams whose original stimulus messages are "keyed in" at an IAFIS workstation (i.e., ITN/FBI), "scanned-in" by an IAFIS scanner (DPS), or input from a magnetic tape or disk are listed as "Internal" to IAFIS.

  In other words, stimuli that are received by wire at the FCE are external to IAFIS, and stimuli that require manual intervention by the FBI or are originated by the FBI within the confines of JEH, Quantico, or the Clarksburg Facility are internal to IAFIS.

Some of the messages represent a collection of several specific messages of that type (e.g., there are several types of latent searches, but only one "aggregate" Search Latent File message is currently defined). This type of additional detail will be incorporated in subsequent versions.

The size of the boxes used to depict processing entities in no way implies the hierarchical relationship between or among the entities. It is simply an expedient to show the interface relationships between each of the pairs of entities.

"Hardcopy Response Data" indicates responses generated by III/FBI that will be sent to originator via the US mail.

The path of a message is depicted by a line indicating origin and destination. You will note that some lines have two arrows facing the same direction: one upon entering the Communication Front End and another at the message's destination. This indicates that the message may be transformed by the Front End. Although transformed, the message's data remains constant. Lines may be labeled with the associated message title, as well as the message's identifying number, facilitating reference to Appendix A and other message tables.

Arrows with dashed lines depict requests that may result in a Rejection Message. Note that the diagrams show User, MRD, and hardcopy input as being potentially rejected for improper format or insufficient data. The diagrams do not show Work Stations as having Rejection Messages spawned (the diagrams depict inter-segment message flow; refer to the ITN/FBI Software Design Document for Text Checks internal to ITN/FBI).

Bi-directional arrows on "Workstation" indicate both input from and output to the workstation.

The diagrams show the flow of data messages between IAFIS Segments, as well as to and from NCIC, the CJIS WAN, and Nlets; refer to the appropriate requirements document for details of the processing logic within the segments.

Redundant numbers indicate that multiple messages may be generated in the same processing step. Refer to the appropriate Segment documentation for details of sequencing requirements and logic.

B.2 Mission-Critical Messages

Ten-Print Services Data Flow

The Ten-Print Services Data Flow Diagrams are representations of IAFIS SRD requirements as

allocated to IAFIS segments by the FBI.

Note

All of the IAFIS Data Flow Diagrams in Appendix B are reproduced electronically from the Message Definition Database (MDD) in an on-line database. They are available only in hard-copy format from IAFIS CM, or may be produced using the MDD tool, also available from CM.

American Standard Code for Information Interchange (ASCII) Characters and Codes

This table defines the printable 7 bit ASCII characters used in many IAFIS elements. These characters include the alphabet (upper and lower case), numbers 0 through 9, and special characters. The printable characters are decimal codes 32 (blank space) through 126 (tilda). If other, non-printable, characters are used, they are explicitly described in the MDD element description.

Binary	Dec	Glyph	Binary	Dec	Glyph
010 0000	32	space	100 1010	74	J
010 0001	33	!	100 1011	75	K
010 0010	34	“	100 1100	76	L
010 0011	35	#	100 1101	77	M
010 0100	36	$	100 1110	78	N
010 0101	37	%	100 1111	79	O
010 0110	38	&	101 0000	80	P
010 0111	39	‘	101 0001	81	Q
010 1000	40	(	101 0010	82	R
010 1001	41	)	101 0011	83	S
010 1010	42	*	101 0100	84	T
010 1011	43	+	101 0101	85	U
010 1100	44	,	101 0110	86	V
010 1101	45	-	101 0111	87	W
010 1110	46	.	101 1000	88	X
010 1111	47	/	101 1001	89	Y
011 0000	48	0	101 1010	90	Z
011 0001	49	1	101 1011	91	{
011 0010	50	2	101 1100	92	|
011 0011	51	3	101 1101	93	}
011 0100	52	4	101 1110	94	^
011 0101	53	5	101 1111	95	_
011 0110	54	6	110 0000	96	`
011 0111	55	7	110 0001	97	a

Binary	Dec	Glyph	Binary	Dec	Glyph
011 1000	56	8	110 0010	98	b
011 1001	57	9	110 0011	99	c
011 1010	58	:	110 0100	100	d
011 1011	59	:	110 0101	101	e
011 1100	60	<	110 0110	102	f
011 1101	61	=	110 0111	103	g
011 1110	62	>	110 1000	104	h
011 1111	63	?	110 1001	105	i
100 0000	64	@	110 1010	106	j
100 0001	65	A	110 1011	107	k
100 0010	66	B	110 1100	108	l
100 0011	67	C	110 1101	109	m
100 0100	68	D	110 1110	110	n
100 0101	69	E	110 1111	111	o
100 0110	70	F	111 0000	112	p
100 0111	71	G	111 0001	113	q
100 1000	72	H	111 0010	114	r
100 1001	73	I	111 0011	115	s
111 0100	116	t	111 1010	122	z
111 0101	117	u	111 1011	123	{
111 0110	118	v	111 1100	124	|
111 0111	119	w	111 1101	125	}
111 1000	120	x	111 1110	126	~
111 1001	121	y			

Figure 21.1-01a External Criminal Ten-Print Submission Data Flow (CAR, CNA, CPNU, DEK) Sequencing and Notes

This DFD applies to the STOTs CAR, CNA, CPNU, and DEK. This data flow illustrates IAFIS processing of the Criminal Ten-Print Answer Required (CAR) Criminal Ten-Print No Answer Necessary (CNA), Criminal Fingerprint Card Processing - Non-Urgent (CPNU), and Known Deceased (DEK) Submissions. If the submissions result in an Ident, the submission data is used to update the existing records in the Criminal Files. If the submission results in a Non-Ident and the submission is to be retained, the submission data is used to create a new record in the Criminal files. The Files used in the process include: 1) the Criminal Ten-Print Fingerprint Image Master File (FIMF) (ITN/FBI), 2) the Ten-Print Certification File (TPCF) (ITN/FBI), 3) the Unsolved Latent Features File (ULF) (AFIS/FBI), 4) the Subject Criminal History File (SCH) (III/FBI), and 5) the Criminal Ten-Print Features Master File (CMF) (AFIS/FBI).

(1) IAFIS receives the EBTS Ten-Print Submission (E1000) message via the CJIS WAN.

When a submission matches the criteria for an iDSM search, EFCON/FBI will send an HTTP message containing the entire submission as a post to the CIPS servers. The subject line of the HTTP message will contain the EFCON/FBI Control Number (ECN) for tracking purposes.

The submission will be forwarded to Automated Quality Check (AQC*). If it passes AQC, processing will move to paragraph 2. AQC can also reject as described below. Otherwise, the ten-print submission will be routed to manual Quality Check (QC) where Service Providers will reject, edit and release, or release the submission. If the submission is rejected by either AQC or a Service Provider, ITN/FBI sends an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.)

(2) If an FBI Number (FNU) is supplied with the Ten-Print submission, ITN/FBI will create an A1227, AFIS Ten-Print Verify and Search message, which will then be routed to AFIS/FBI. This message contains the FILE-HANDLE that AFIS/FBI will use to retrieve the file containing the fingerprint submission images from ITN/FBI, formatted in accordance with I3220.

When AFIS/FBI receives the A1227 message, AFIS/FBI will assess the submitted fingerprint image quality, after which AFIS/FBI will perform Automated Sequence Check (ASC). If the quality of the fingerprint images is acceptable for search but not high enough quality to be retained in the repository, a Search But Don't Add (SBDA) indicator is set by AFIS/FBI. If the quality is assessed as too low for searching, the transaction will be immediately routed back to ITN/FBI with an A1802, and ITN/FBI will send an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.) If ASC is successful, the fingerprint features are written to a file to be utilized for potential file maintenance.

If ASC is not successful, AFIS/FBI will send an AFIS Ten-Print Verify and Search Response Data Candidate List (A1222) with the ASC_PASS=N. ITN/FBI will then route the submission to manual Fingerprint Sequence Check (FSC) for processing. The FSC Service Provider may release the transaction, swap the fingerprint images and release the transaction, place stamps on the fingerprint images and release the transaction or reject the submission. If the submission is rejected, ITN/FBI sends an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.) If the FSC Service Provider releases the transaction, ITN/FBI will route the transaction to a Quality Assurance FSC (QA-FSC) Service Provider who will review the FSC decision. If the QA-FSC Service Provider releases the transaction, ITN/FBI will resend the A1227 message to AFIS/FBI with the Perform_ASC= N.

* For information on AQC, see the ISDD Design Note #25

If FNUs are supplied in the A1227 message, either as a result of quoted FNUs or as a result of the III subject search, AFIS/FBI will perform a one–to-one compare against the stored feature vectors. If the match score is below the "no match" threshold, the quoted FNUs or the FNUs provided through the subject search are considered to be not viable candidates and AFIS/FBI will initiate a feature search of the CMF.

NOTE: ITN/FBI sets the 2nd Look Flag and the QA Eligibility Flag based on thresholds and the match score of the candidates. For more information on these flags, see the ITN SwDD Section 3.2.2.7.

Or

(3) If an FNU is not supplied with the Ten-Print submission, ITN/FBI will initiate a subject search by sending the Subject Search Request (A1030) message to III/FBI. This subject search is performed against the Subject Criminal History File which could produce a list of FNUs (candidate list).

(4) III/FBI will perform filtering and return the results to ITN/FBI in a Ten-Print Subject Search Request Response (A1031). For ITN/FBI handling of special subjects (Stops or Wants SPF or AUD values) refer to IAFIS System Design Document (ISDD), Design Note #17.

NOTE: ITN/FBI sets the 2nd Look Flag when the III subject search candidate matches on Name, DOB, and SOC (CAND_TYPE = 2).

(5) ITN/FBI will create an AFIS Ten-Print Verify and Search message (A1227) containing the candidate FNUs supplied by the III subject search. ITN/FBI routes the A1227 message to AFIS/FBI (Perform_ASC=Y). (Note: AFIS/FBI will process the A1227 as in step 2.)

(6) AFIS/FBI will return the AFIS Ten-Print Verify and Search Response Data Candidate List (A1222) message to ITN/FBI. If the A1222 message contains candidates, ITN/FBI will retrieve the candidate images, and the transaction will be staged for a Fingerprint Image Comparison (FIC) Service Provider.

(7) If filtering reveals a subject record containing AUD= 'T,' ITN/FBI will route the transaction to the appropriate location based on the SPF code (SPF='T' will be routed to Wants, all other SPF values will be routed to Special Stops). In these instances, ITN/FBI will pre-stage the desired criminal histories using the A1032/A1033 message pair.

Fingerprint Image Comparison (FIC) indicator levels, which are returned by AFIS/FBI in the A1222 message, are used by ITN to determine the number of manual FICs needed. A FIC indicator level of 100 requires no manual FIC operations. A FIC indicator level of 101 requires one manual FIC operation. A FIC indicator level of 102 requires two manual FIC operations.

If the FIC indicator level is 102, the first FIC Service Provider may Ident the submission, Non-Ident the submission, or reject the submission. If this Service Provider rejects the submission, ITN/FBI sends an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.) If the Service Provider Non-Idents the submission and the 2nd Look Flag is true, the submission will be routed to FIC Evaluation Review (Eval); otherwise if the QA Eligibility Flag is true the submission is routed to QA-FIC. If either the Eval or the QA-FIC Service Provider Non-Ident the submission, then ITN/FBI determines if a feature search has been performed. If it has not, ITN/FBI will send an A1227 message without candidates and processing will proceed from that point (step 8). (If AFIS/FBI has cascaded a feature search of the CMF, processing will continue in step 9) If the first FIC Service Provider Idents the submission, the submission moves to a second FIC Service Provider. If the second FIC Service Provider Idents the submission and the QA Eligibility Flag is true, the submission is routed to QA-FIC. If the second FIC Service Provider or the QA-FIC Service Provider either Non-Idents or rejects a submission which the first FIC Service Provider Idented, the submission is routed to Eval for evaluation of the discrepancy. If the QA-FIC or Eval Service Provider Idents the submission, then it is routed to file maintenance (See paragraph 11). If the Eval Service Provider rejects the submission, ITN/FBI sends an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI

which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.)

If the FIC indicator level is 101 the FIC Service Provider may Ident the submission, Non-Ident the submission, or reject the submission. If the FIC Service Provider Idents the submission and the QA Eligibility Flag is true, the submission is routed to QA-FIC. If the QA-FIC Service Provider Idents the submission, then it is routed to file maintenance (See paragraph 11). If the FIC Service Provider or QA-FIC Service Provider Non-Idents or rejects the submission, the submission is routed to the Eval for evaluation of the discrepancy. If the Eval Service Provider Idents the submission, then it is routed to file maintenance (See paragraph 11). If the Eval Service Provider rejects the submission, ITN/FBI sends an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.) If the Eval Service Provider Non-Idents the submission, then ITN/FBI determines if a feature search has been performed. If it has not, ITN/FBI will send an A1227 message without candidates and processing will proceed from that point. (If AFIS/FBI has cascaded a feature search of the CMF, processing will continue in step 9)

If the FIC indicator level is 100 and the QA Eligibility Flag is true, the transaction is routed to QA-FIC. If the decision is Non-Ident or reject, then the submission will be forwarded to Eval for a final decision. If the QA-FIC or Eval Service Provider Idents the submission, then it is routed to file maintenance (See paragraph 11). If the Eval Service Provider rejects the submission, ITN/FBI sends an A1801 to III/FBI which formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.) If the Eval Service Provider Non-Idents the submission, then ITN/FBI determines if a feature search has been performed. If it has not, ITN/FBI will send an A1227 message without candidates and processing will proceed from that point (step 8). (If AFIS/FBI has cascaded a feature search of the CMF, processing will continue in step 9) If the QA Eligibility flag is false, then the submission is routed to file maintenance (see paragraph 11 for details) as an Ident.

NOTE: If a feature search has been performed but no III subject search has been perform then ITN/FBI will send an A1030 (step 3).

(8) If the previous steps have not produced an Ident to the submitted subject (Quoted FNUs or Subject Search Candidates) and no feature search has been performed, ITN/FBI will send the AFIS Ten-Print Verify and Search (A1227) message (Perform_ASC=N) to AFIS/FBI where a ten-print search is performed against the CMF. This message contains the FILEHANDLE which AFIS/FBI will use to retrieve the file containing images from ITN/FBI, formatted in accordance with I3220.

(9) AFIS/FBI will return all candidates to ITN/FBI in the A1222 message. ITN/FBI will retrieve the candidate images and stage the submission for Service Provider FIC. Processing will continue as described in paragraph 7.

NOTE: If the submission has resulted in multiple Idents, Eval must confirm the Idents before IAFIS spawns Consolidation processing (Refer to 21.3-02). This spawned process performs consolidation file maintenance in III/FBI and then returns to this point to perform ten-print file maintenance.

(10) The Search Status for Non-Ident and Rejection Ten-Print Submissions (A3314) message will be sent to AFIS/FBI when a Non-Ident or reject occurs on any candidates for a ten-print submission for which the **last** AFIS fingerprint search produced candidates. No response from AFIS/FBI is required.

(11) ITN/FBI sends the Ten-print Criminal History File Maintenance Request (A3026) message to III/FBI to add a new FNU or update an existing FNU. If the submission has updated an existing FNU, III/FBI will perform filtering and update the Subject Criminal History File. If filtering reveals a Special Stops subject, and the transaction has not been reviewed by the Special Stops Unit, III will reject A3026 with an A1802 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. **If the Special Stops review results in a decision to Non-Ident the candidate with the submission, no A3314 will be sent.** Upon completion of the review (the Special Stops Service Provider releases the transaction from the stops log), ITN/FBI will resend A3026.

NOTE: If the A3026 tries to update a record containing a Want, III/FBI sends a Deceased (for DEK) or Non-Deceased (for CAR, CNA, and CPNU) Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) message to the Want originator. III/FBI will also send an A1312 Review Request message to ITN/FBI for Answer Hits to Wants (AHTW) notification. When AHTW is finished with the review, ITN/FBI will send an A1313 Review Response to III/FBI. III/FBI then proceeds to perform response generation.

NOTE: If the A3026 updates a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Notice(s) via an SOR Agency Notice (N3126) message to all registering agencies.

(12) If the A3026 tries to update a record with a Flash, III/FBI will print an IDRR, which will be sent to the Flash originator.

The following subset of messages applies to completing the submission response when the FBI is responsible for collecting and disseminating NFF-maintained data.

(13) If the subject record (from an Idented submission) contains active NFF state pointers, III/FBI will send an N3105 message via NCIC to any states that have a criminal history on the subject.

(14) III/FBI will queue the FBI portion of the response until the state criminal history data is returned in the Nlets CR Response (L1048) message. III/FBI will code the A1003 with an electronic rap sheet (ERS) containing the FBI-held portion of the record together with the criminal history data received from the NFF states (L1048).

If the NFF state(s) does not respond within the allowable criminal response parameters, or if the NFF state(s) provides an incomplete response, III/FBI will code the A1003 containing the FBI portion of the record and any retrieved data from the NFF state(s) sending the message to ITN/FBI.

If an Ident occurred against a file record identified as an unknown deceased person, III/FBI will also prepare an IDRR for the owner of the unknown deceased person record.

If the submission hits to a Want/Flash, the Want/Flash information will be included in the response.

(15) If the TOT is CAR, CPNU, or DEK, the Ten-Print Submission Response (A1003) message is sent to ITN/FBI which converts it to an E1003 and forwards it to EFCON which will send the message to the contributor via the CJIS-WAN.

(16) If a Special Stops Service Provider requires the hardcopy response to be redirected from III/FBI to a Special Stops printer in ITN/FBI (ONC = 'R' in A3026), III/FBI will send an Unsolicited Report (A3150) message containing the IDRR/NIDR to ITN/FBI to be printed on the Special Stops printer.

The following is a list of unsolicited reports that may be sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
IDRR/NIDR	Answer Hits to Wants
IDRR/NIDR	Special Stops

The following subset of message flows applies to completing the file maintenance process.

*****III/FBI generates and sends a QTP Request Message to NCIC follow-**

ing the start of File Maintenance and after the completion of any required manual reviews.

(17) III/FBI returns the Ten-Print File Maintenance Response (A3025) message to ITN/FBI. Upon receipt of the A3025, ITN/FBI initiates the file maintenance processes of ten-print certification file add, and a FIMF add/update. If the result of the Non-Retain submission is a Non-Ident, ITN/FBI will spawn Cascaded ULF search Processing (as described in Figure F21.1-10)

(18) ITN/FBI sends the Add/Update Fingerprint Features Request (A3310) message to AFIS/FBI. A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI in accordance with formatting per I3020. For an Ident, AFIS/FBI updates features, if better, and descriptive information in the Criminal Master File (CMF). For a criminal Non-Ident retain, AFIS/FBI creates a new criminal record. If the submission resulted in a Criminal Non-Ident Retain or in a Criminal Ident with upgraded features, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

(19) AFIS/FBI will respond to A3310 with the Update Fingerprint Features Response (A3311) message.

(20) ITN/FBI will store submissions in the Ten-Print Certification File if the submission is an Ident or the submission is a Non-Ident criminal retained submission. The Ten-Print Certification File Index and the pattern classification (provided by AFIS/FBI) are sent to III/FBI via the File Maintenance Completion Notification (A3331) message. If the file maintenance process has completed successfully and further Service Provider review of the submission is not needed, ITN/FBI will close out the submission.

(21) If the submission contained mug shot photos of the criminal subject (one or more T10 records were received in the E1000), ITN/FBI will write the photo image data to an I1001 format file and send the Ten-Print Photo File Maintenance Request (A3024) message to III/FBI. III/FBI uses the included FNU and arrest cycle to link the photo to the subject arrest and uses FILEHANDLE to retrieve the file containing the photo images from ITN/FBI. III/FBI will also update the associated record with an SPF = 'E' to indicate that a photo(s) is on file for this arrest.

(22) III/FBI will respond to A3024 with the File Maintenance Response (A3027) message.

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3401 Hit to Want Notification
N3107 Unsolicited Deceased Notification
N3112 Multi-state Offender Status
N3114 Non-matching SID Ignored
N3115 No Prior Record – SID Entered
N3116 Prior Record – Previously Entered SID Notification (Single)
N3117 Prior Record – SID Entered
N3119 Reject, No Prior Record, SID Not Entered
N3120 Reject, Prior Record, SID Not Entered
N3123 Prior Record – Previously Entered SID (Multi)
N3126 SOR Agency Notice

Figure 21.1-01b External Civil Ten-Print Submission Data Flow (EMUF, FANC, FAUF, NFAP, NFUE, NFUF, MAP, and DOCE) Sequencing and Notes

This DFD applies to the STOTs FANC, FAUF, NFAP, NFUF, NFUE, MAP and DOCE. This data flow illustrates IAFIS processing of the Civil Ten-print Federal Applicant No Charge (FANC), Federal Applicant User Fee (FAUF), Non-Federal Advanced Payment (NFAP), Non-Federal Applicant User Fee (NFUF), Non-Federal User Fee Expedite (NFUE), Miscellaneous Applicant Civil (MAP) and Departmental Order Channeling Electronic (DOCE) Submissions. If the submission results in an Ident, the data is used to update existing records in the Criminal Files. If the submission results in a Non-Ident and the submission is to be retained, the data is used to create new records in the Civil Files. The Files used in the process include: 1) the Criminal Ten-print Fingerprint Image Master File (FIMF) (ITN/FBI), 2) the Ten-print Certification File (TPCF) (ITN/FBI), 3) the Subject Criminal History (SCH) File (III/FBI), 4) the Civil Subject Index Master File (III/FBI), 5) the Criminal Ten-print Features Master File (CMF) (AFIS/FBI), 6) the Civil On-line Features File (AFIS/FBI), and 7) the Civil Ten-print Online Image File (ITN/FBI).

(1-10) Processing progresses as described in Figure 21.1-01a to this point.

(11) If the retain submission resulted in a Non-Ident, ITN/FBI will send a Ten-print Civil Subject File Maintenance Request (A3340) to III/FBI. The A3340 message will request that a record be added to the Civil Subject Index Master File.

(12) If the submission resulted in an Ident, ITN/FBI sends the Ten-print Criminal History File Maintenance Request (A3026) message to III/FBI to update an existing FNU. If the submission has updated an existing FNU, III/FBI will perform filtering and update the Subject Criminal History File. If filtering reveals a Special Stops subject and the transaction has not been reviewed by the Special Stops Unit, III will reject A3026 with an A1802 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. **If the Special Stops review results in a decision to Non-Ident the candidate, with the submission, no A3314 will be sent.** Upon completion of the review (the Special Stops Service Provider releases the transaction from the stops log), ITN/FBI will resend A3026.

NOTE: If the A3026 tries to update a record containing a Want, III/FBI sends a Non-Deceased Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) message to the Want originator. III/FBI will also send an A1312 Review Request message to ITN/FBI for Answer Hits to Wants (AHTW) notification. When AHTW ITN/FBI is finished with the review, ITN/FBI will send an A1313 Review Response to III/FBI. III/FBI then proceeds to perform response generation.

NOTE: If the A3026 updates a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Notice(s) via an SOR Agency Notice (N3126) message to all registering agencies.

(13) If the A3026 updates a record with a Flash, III/FBI will print an IDRR, which will be sent to the Flash originator.

NOTE: If the STOT is EMUF, the system will generate a hardcopy rap sheet to be mailed to all CRIs included in the submission.

The following subset of messages applies to completing the submission response when the FBI is responsible for collecting and disseminating NFF-maintained data.

(14) If the subject record (from an Idented submission) contains active NFF state pointers, III/FBI will send an N3105 message via NCIC to any states that have a criminal history on the subject.

(15) III/FBI will queue the FBI portion of the response until the state criminal history data is returned in the Nlets CR Response (L1048) message. III/FBI will code the A1003 with an electronic rap sheet (ERS) containing the FBI portion of the record together with the criminal history data received from the NFF states (L1048). If the NFF state(s) does not respond within the allowable criminal response parameters, or if the NFF state(s) provides an incomplete response, III/FBI will code the A1003 containing the FBI portion of the record and any retrieved data from the NFF state(s) and will return the message to ITN/FBI.

If an Ident occurred against a file record identified as an unknown deceased person, III/FBI will also prepare an IDRR for the owner of the unknown deceased person record.

If the submission hits to a Want/Flash, the Want/Flash information will be included in the response.

(16) The Ten-Print Submission Response A1003 message is sent to ITN/FBI which converts it to an E1003 and forwards it to the contributor; the E1003 is sent to EFCON which will send the message to the contributor via the CJIS-WAN.

NOTE: For EMUF Submissions: the Ten-Print response through EFCON will only include the SRE; the hardcopy rap sheet will be mailed separately (see NOTE under (13) above).

(17) If a Special Stops Service Provider requires the hardcopy response to be redirected from III/FBI to a Special Stops printer in ITN/FBI (ONC = 'R' in A3026), III/FBI will send an Unsolicited Report (A3150) message containing the IDRR/NIDR to ITN/FBI to be printed on the Special Stops printer.

The following is a list of unsolicited reports that may be sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
IDRR/NIDR	Answer Hits to Wants
IDRR/NIDR	Special Stops

The following subset of message flows applies to completing the file maintenance process.

*****III/FBI generates and sends a QTP Request Message to NCIC following the start of File Maintenance and after the completion of any required manual reviews.**

(18) III/FBI returns the Ten-Print File Maintenance Response (A3025) message to ITN/FBI. Upon receipt of the A3025, ITN/FBI initiates the file maintenance processes of ten-print certification file add and a FIMF add/update.

(19) ITN/FBI sends the Add/Update Fingerprint Features Request (A3310) message to AFIS/FBI. A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI formatted in accordance with I3020. For an Ident, AFIS/FBI updates features, if better, and descriptive information in the Criminal Master File; for a Civil Non-Ident retain, AFIS/FBI creates a new civil record. If the submission resulted in a Criminal Ident with upgraded features, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

(20) AFIS/FBI will respond to A3310 with the Update Fingerprint Features Response (A3311) message.

(21) ITN/FBI will store submissions in the Ten-Print Certification File only if the submission is a Criminal Ident. The Ten-Print Certification File Index and the pattern classification (provided by AFIS/FBI) are sent to III/FBI via the File Maintenance Completion Notification (A3331) message. If the file maintenance process has completed successfully and further Service Provider review of the submission is not needed, ITN/FBI will close out the submission.

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3401 Hit to Want Notification
N3102 No Prior Record Civil (CFN)
N3103 Prior Record Civil (CFR)
N3107 Unsolicited Deceased Notification
N3112 Multi-state Offender Status
N3114 Non-matching SID Ignored
N3115 No Prior Record – SID Prior Record – SID Entered
N3116 Prior Record – Previously Entered SID Notification (Single)
N3117 Prior Record – SID Entered
N3119 Reject, No Prior Record, SID Not Entered
N3120 Reject, Prior Record, SID Not Entered
N3123 Prior Record – Previously Entered SID (Multi)
N3126 SOR Agency Notice

Figure 21.1-01c External Humanitarian Ten-Print Submission Data Flow (DEU, MPR, AMN) Sequencing and Notes

This DFD applies to the STOTs DEU, MPR, and AMN. This data flow illustrates IAFIS processing of Ten-print Unknown Deceased (DEU), Missing Person (MPR), and Amnesia Victim (AMN) Submissions. These submissions are accepted by the FBI for humanitarian reasons. The feature that distinguishes these submissions is that the process of attempting an Ident includes searching the civil files in addition to the criminal files. The civil search is performed if the submission is a Non-Ident in the criminal file. If the submission results in an Ident against the Criminal Files, the data is used to update the existing criminal record. If the submission results in a Non-Ident and the submission is to be retained, the data is used to create new records in the Criminal Files. If the submission results in an Ident against the Civil Files, the data is used to create new records in the Criminal Files with the response containing the civil identification. The files included in the process are: 1) the Criminal Ten-print Fingerprint Image Master File (FIMF) (ITN/FBI), 2) the Ten-print Certification File (TPCF) (ITN/FBI), 3) the Subject Criminal History File (SCH) (III/FBI), 4) the Civil Subject Index Master File (III/FBI), 5) the Criminal Ten-print Features Master File (CMF) (AFIS/FBI), 6) the Civil On-line Features File (AFIS/FBI), and 7) the Civil Ten-Print On-Line Image File (ITN/FBI) (for comparison).

(1-10) Processing progresses as described in Figure 21.1-01a to this point with one exception, only the MPR performs a subject search (A1030); AMN and DEU will proceed directly to the A1227 message. And no A3314 message will be sent (step 10)

(11) If Non-Ident results from Criminal File searches and the TOT is MPR in the ten-print submission, a Ten-Print Subject Search (A1030) message will be sent to III/FBI initiating a search against the Civil Subject Index Master File. The value of NDR (Name of the Designated Repository) in message will be set to '2' (NDR=2).

(12) III/FBI will return the Ten-print Subject Search Request Response (A1031) message which may contain a list of Civil Record Numbers (CRN).

(13) If a Non-Ident results from Criminal File searches and the TOT is AMN or DEU, an A1227 message is formulated by ITN/FBI and sent to AFIS/FBI with NDR=2. A1227 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI, formatted in accordance with I3220.

(14) The results from flow (13) are placed in the A1227 message to be sent to AFIS/FBI. If CRNs are supplied in the A1227 message, as a result of the III subject search (A1031), AFIS/FBI will perform a one-to-one compare against the stored feature vectors. If the match score is below the "no match" threshold, the CRNs provided through the subject search are considered not to be viable candidates and AFIS/FBI will initiate a feature search of the Civil On-Line Features File (NDR=2). A1227 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI, formatted in accordance with I3220. AFIS/FBI will respond with the AFIS Search Response Candidate List (A1222) message.

(15) AFIS/FBI will return the AFIS Ten-Print Verify and Search Response Data Candidate List (A1222) message to ITN/FBI. If the A1222 message contains candidates, processing will continue as described in Figure 21.1-01a, paragraph 4.

(16) The message Search Status for Non-Ident Ten-Print Submissions (A3314) message will be sent to AFIS/FBI when a Non-Ident or reject occurs for a ten-print submission for which the last AFIS fingerprint search produced candidates. No response from AFIS/FBI is required.

(17) ITN/FBI sends the Ten-print Criminal History File Maintenance Request (A3026) message to III/FBI to add a new FNU or update an existing FNU. If the submission has updated an existing FNU, III/FBI will perform filtering and update the Subject Criminal History File. If filtering reveals a Special Stops subjects, and the transaction has not been reviewed by the Special Stops Unit, III will reject A3026 with an A1802 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. **If the Special Stops review results in a decision to non-Ident the candidate with the submission, no A3314 will be sent.** Upon completion of the review (the Special Stops Service Provider releases the

transaction from the stops log), ITN/FBI will resend A3026.

NOTE: If the A3026 tries to update a record containing a Want, III/FBI sends a Deceased (for DEU) or Non-Deceased (for MPR and AMN) Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) message to the Want originator. III/FBI will also send an A1312 Review Request message to ITN/FBI for Answer Hits to Wants (AHTW) notification. When AHTW ITN/FBI is finished with the review, ITN/FBI will send an A1313 Review Response to III/FBI. III/FBI then proceeds to perform response generation.

NOTE: If the A3026 updates a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Notice(s) via an SOR Agency Notice (N3126) message to all registering agencies.

(18) If the A3026 updates a record with a Flash, III/FBI will print an IDRR, which will be sent to the Flash originator.

The following subset of messages applies to completing the submission response when the FBI is responsible for collecting and disseminating NFF-maintained data.

(19) If the subject record (from an Idented submission) contains active NFF state pointers, III/FBI will send an N3105 message via NCIC to any states that have a criminal history on the subject.

(20) III/FBI will queue the FBI portion of the response until the state criminal history data is returned in the Nlets CR Response (L1048) message. III/FBI will code the A1003 with an electronic rap sheet (ERS) containing the FBI-held portion of the record together with the criminal history data received from the NFF states (L1048). If the NFF state(s) does not respond within the allowable criminal response parameters, or if the NFF state(s) provides an incomplete response, III/FBI will code the A1003 containing the FBI portion of the record and any retrieved data from the NFF state(s) and sends the message to ITN/FBI.

If an Ident occurred against a file record identified as an unknown deceased person, III/FBI will also prepare an IDRR for the owner of the unknown deceased person record.

If the submission hits to a Want/Flash, the Want/Flash information will be included in the response.

(21) The Ten-Print Submission Response A1003 message is sent to ITN/FBI which converts it to an E1003 and forwards it to the contributor; the E1003 is sent to EFCON which will send the message to the contributor via the CJIS-WAN.

(22) If a Special Stops Service Provider requires the hardcopy response to be redirected from III/FBI to a Special Stops printer in ITN/FBI (ONC = 'R' in A3026), III/FBI will send an Unsolicited Report (A3150) message containing the IDRR/NIDR to ITN/FBI to be printed on the Special Stops printer.

The following is a list of unsolicited reports that may be sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
IDRR/NIDR	Answer Hits to Wants
IDRR/NIDR	Special Stops

The following subset of message flows applies to completing the file maintenance process.

*****III/FBI generates and sends a QTP Request Message to NCIC following the start of File Maintenance and after the completion of any required manual reviews.**

(23) III/FBI returns the Ten-Print File Maintenance Response (A3025) message to ITN/FBI. Upon receipt of the A3025, ITN/FBI initiates the file maintenance processes of TPCF add and a FIMF add/update.

(24) ITN/FBI sends the Update Fingerprint Features Request (A3310) message to AFIS/FBI. A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI formatted in accordance with I3020. For an Ident, AFIS/FBI updates features, if AFIS/FBI or a FIC or FSC Service Provider determines them to be better, and descriptive information in the Criminal Master File; for a criminal Non-Ident retain, AFIS/FBI creates a new record. If the submission resulted in a Criminal Non-Ident Retain or in a Criminal Ident with upgraded features, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

(25) AFIS/FBI will respond to A3310 with the Update Fingerprint Features Response (A3311) message.

(26) ITN/FBI will store submissions in the TPCF only if the submission is an Ident or if a criminal retained submission is a Non-Ident. The TPCF Index and the pattern classification (provided by AFIS/FBI) are sent to III/FBI via the File Maintenance Completion Notification (A3331) message. If the file maintenance process has completed successfully and further Service Provider review of the submission is not needed, ITN/FBI will close out the submission.

(27) If the submission contained mug shot photos of the criminal subject (one or more T10 records were received in the E1000), ITN/FBI will write the photo to image data to an I1001 format file and send the Ten-Print Photo File Maintenance Request (A3024) message to III/FBI. III/FBI uses the included FNU and arrest cycle to link the photo to the subject arrest, and FILEHANDLE to retrieve the file containing the photo images from ITN/FBI. III/FBI will also update the associated record with an SPF = 'E' to indicate that a photo(s) is on file for this arrest.

(28) III/FBI will respond to A3024 with the File Maintenance Response (A3027) message.

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3401 Hit to Want Notification
N3102 No Prior Record – Civil (CFN)
N3103 Prior Record – Civil (CFR)
N3107 Unsolicited Deceased Notification
N3112 Multi-state Offender Status
N3114 Non-matching SID Ignored
N3115 No Prior Record – SID Entered
N3116 Prior Record – Previously Entered SID Notification (Single)
N3117 Prior Record – SID Entered
N3119 Reject, No Prior Record, SID Not Entered
N3120 Reject, Prior Record, SID Not Entered
N3123 Prior Record – Previously Entered SID (Multi)
N3126 SOR Agency Notice

Figure 21.1-01d Card Scanning Service T/P Submission Supplemental Data Flow Sequencing and Notes

The data flow applies to the following STOTs: CARC (Criminal Ten-Print Submission (Answer Required)), CNAC (Criminal Ten-Print CSS Submission (No Answer Required)), DEKC (Known Deceased CSS Submission), FCMA (Federal Applicant MRD Submission (No Chg)), FNCC (Federal Applicant CSS Submission, (No Charge)) FUFC (Federal Applicant CSS Submission (User Fee)), MAPC (Miscellaneous Applicant CSS Submission (No Charge)), NFDP (Non-Federal Applicant CSS Submission (User Fee-Direct Payment)), and NFFC (Non-Federal Applicant CSS Submission (User Fee)). (Note that the exclusion of STOTs AMN, DEU, and MPR is intentional. These cards will not be processed through the Card Scanning Service (CSS) facility but will be sent to the FBI and processed by DPS.) This data flow illustrates the message sequence for those messages specific to processing submissions received through the CSS facility and transmitted to IAFIS via the CJIS WAN. The messages shown here are supplemental to the External Ten-print Submission Data Flow diagrams 21.1-01a; that is, these processing flows will take place in the context of any Ten-print submission process when the electronic submission is initiated at the CSS. The interaction with the CSS is being shown here rather than on each of the individual Ten-Print submission diagrams to avoid confusion.

NOTE: FCMA enters the system thru CSS but is converted to FANC by EFCON

NOTE: (a) Non-CSS NFFC submissions will be converted to the STOT EMUF by EFCON (Refer to Figure 21.1.01b for EMUF Data Flow Sequencing and Notes)

(b) All other agencies desiring hardcopy responses from electronic submissions must utilize the EMUF STOT.

(1) The EBTS Ten-Print Submission (E1000) message is received by EFCON via the CJIS WAN, and then sent to ITN/FBI. The TOTs carried by E1000 as depicted in this diagram will be unique to the CSS (refer to the E1000 message definition and the TOT Code Table, contained in the IAFIS MDD).

If the image quality is acceptable, card data is complete and the scan operation is successful, normal Ten-Print submission processing proceeds (see DFDs 21.1-01a).

NOTE: If the A3026 tries to update a record containing a Want, III/FBI sends a Non-Deceased (for CARC and CNAC) Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) to the Want Originator and the Arresting Agency. III/FBI sends a Deceased Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) to the Want Originator only (No Arresting Agency Notification is sent) when the submission is deceased (DEKC).

(2) If the image quality is unacceptable, card data is incomplete, or the scan operation is unsuccessful, normal processing is terminated and ITN/FBI sends an EBTS Error Response Request (A1801) message to III/FBI.

(3) III/FBI formats the Card Disposition Response (A1001) message and sends the message to ITN/FBI which converts it to an E1001 and forwards it to EFCON which will send the message to CSS via the CJIS WAN. This informs the CSS that the transaction is complete and that the hard copy can be dispositioned according to the disposition code (CDDISP). The response to the CSS is generated simultaneously with the appropriate response in hard copy format that III/FBI produces and sends to the submitter via mail.

(4) If ITN/FBI initiates A1801, III/FBI formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS WAN. (Refer to DFD 21.6-01 for error processing detail.) This message notifies the CSS of transaction failure. If the problem can be corrected by the CSS (card rescan, etc.), the transaction is reinitiated. If a problem exists with the hard copy, CSS rejects the submission to the submitter.

If a transaction originating at the CSS is rejected, the CSS staff may elect to initiate a resubmission. This will be done by manually entering ALL of the data from the card, rescanning, and sending an E1000 using the appropriate Type-2 resubmit TOT.	Message Number/Name N3401-Unsolicited Hit to Want Notification

Figure 21.1-02a Internal Ten-Print Submission Data Flow Sequencing and Notes

This diagram applies to the following STOTs: , IAMN, ICAR, ICNA, IDEK, IDEU, IFANC, IFAUF, IMAP, IMPR, and INFUF. . This diagram illustrates IAFIS processing of internal ten-print submissions. Very low volume hardcopy fingerprint cards (IAMN, IDEU, IMPR and other special cases) handled directly by ITN/FBI are considered internal submissions. If the submissions result in an Ident, the submission data is used to update the existing records in the Criminal Files. If the submission results in a Non-Ident and the submission is to be retained, the submission data is used to create a new record in the Criminal files. The Files used in the process include: 1) the Criminal Ten-Print Fingerprint Image Master File (FIMF) (ITN/FBI), 2) the Ten-Print Certification File (TPCF) (ITN/FBI), 3) the Unsolved Latent Fingerprint Image File (ULF) (ITN/FBI), 4) the Subject Criminal History File (SCH) (III/FBI), and 5) the Criminal Ten-Print Features Master File (CMF) (AFIS/FBI).

The 'ITN Workstation' arrows represent scanning and entering data for the very low volume of hardcopy fingerprint cards at an ITN/FBI workstation.

(1) ITN/FBI will initiate a subject search by sending the Subject Search Request (A1030) message to III/FBI and will include the supplied FNU (if available).

(2) If a supplied FNU has been killed as the result of a previous consolidation and the kept FNU was not returned as a candidate from the subject search, III/FBI will include the associated kept FNU in the Ten-Print Subject Search Response (A1031) message. This subject search is performed against the SCH File which produces a list of FBI Numbers (candidate list). The subject of a supplied FNU will also be returned as a candidate. III/FBI will perform filtering. For ITN/FBI handling of special subjects (Stops or Wants SPF or AUD values) refer to IAFIS System Design Document (ISDD), Design Note #17.

(3) If filtering reveals a subject record containing AUD = 'T,' ITN/FBI will route the transaction to the appropriate location based on the SPF code. In these instances, ITN/FBI will pre-stage the desired criminal histories using the A1032/A1033 message pair.

(4) If an Non-Ident has resulted from the preceding subject search, ITN/FBI will send the AFIS Ten-print Search (A1027) message to AFIS/FBI to initiate a search of the Criminal Ten-print Features File. A1027 contains the FILE-HANDLE which AFIS/FBI will use to retrieve the file containing images from ITN/FBI. The file is formatted per I3020. **Ten-print submissions with STOTs of IAMN and IDEU proceed directly to the AFIS Ten-print search (flows (5) and (6)).**

(5) AFIS/FBI will respond with the AFIS Search Response Data Candidate List (A1022) message.

NOTE: If the submission resulted in multiple criminal Idents, at this point Consolidation processing will take place and returns to this DFD to perform ten-print file maintenance.

(6) For submissions resulting in non-Ident against the criminal file, **IMPR submissions only** will perform a Civil subject search (A1030)

(7) III/FBI will respond with an Ten-Print Subject search Response (A1031), ,

(8) For **IAMN, IMPR, and IDEU submissions only** a second fingerprint search (A1027) against the civil files will be performed at the conclusion of criminal file searches.

(9) AFIS/FBI will return the AFIS Search Response Data Candidate List (A1022). The FBI will retain unidentified submissions (AMN, DEU, and MPR) in the criminal files for possible future identification.

(10) If Ident to Criminal or Criminal Retain Non-Ident ITN/FBI sends the Ten-Print Criminal History File Maintenance Request (A3026) message to III/FBI. For a Criminal Ident, III performs filtering that reveals the following.

a) With a Special Stop subject (SPF = '5' or '6'' or 'C' or 'N') where the transaction has not been reviewed by the Special Stops Unit, III/FBI will reject A3026 for Unauthorized Access with an A1802. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review; the Special Stops Service Provider will complete the transaction

Or;

b) With an SPF = 'K' where the transaction has not been reviewed by DOC SPEC, III/FBI will reject A3026 for Unauthorized Access with an A1802. When this rejection occurs, ITN/FBI will route the transaction to DOC SPEC for review. Upon completion of the review, ITN/FBI will resend A3026.

(11) For civil/Retain Non-Ident ten-print submissions, a Ten-Print Civil Subject File Maintenance Request (A3340) message will be sent from ITN/FBI to III/FBI.

The following subset of message flows applies to completing the submission response.

(12) To compile the response to an Ident if active NFF state pointers are in the record, III/FBI may send an Unsolicited Criminal History Request (N3105) message via NCIC and

(13) III/FBI will receive the response(s) via Nlets (L1048).

If the A3026 attempted to update a record containing a Want and if this is a civil submission, III/FBI suspends the hard copy response generation and processing proceeds in parallel with paragraphs 14 and 18.

(14) If this occurs, III/FBI will generate a Review Request (A1312) message that will be routed to AHTW for review and processing. Civil hits to Wants result in Service Provider phone contact with the Want originator.

(15) The Service Provider may release the transaction for response generation after the review. The result of the AHTW review is a Review Response (A1313) message sent from ITN/FBI to III/FBI.

NOTE: If the submission is civil, the A1313 may direct III/FBI to send a Non-Deceased Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) to the Want Originator.

NOTE: If a criminal submission hits to a Want, the preceding Review Request and Response are omitted and III/FBI sends a Non-Deceased Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) to the Want Originator and the Arresting Agency. III/FBI sends a Deceased Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) to the Want Originator only (no arresting agency notification is sent) when the submission is deceased.

NOTE: If the A3026 updates a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) message to all registering agencies. III/FBI then proceeds to perform response generation.

(16) Responses to the very low volume hardcopy submissions are printed by III/FBI. If a Service Desk provider or Special Stops provider is processing the action, III/FBI may redirect the hardcopy response to ITN/FBI (ONC = 'R' or TOO = 'W') via an Unsolicited Report (A3150) message containing the IDRR/NIDR.

(17)For a criminal submission, if A3026 tries to update a record with a Flash, III/FBI will print an IDRR, which will be sent to the Flash originator.

The following subset of message flows applies to completing the file maintenance process.

(18) III/FBI responds to either the A3026 or the A3340 with the Ten-Print File Maintenance Response (A3025), triggering the ITN/FBI update to the Fingerprint Image Master File and to start the update with AFIS/FBI. A3025 also triggers the update of the Ten-Print Certification File for additions or updates to the criminal files.

(19) ITN/FBI sends an Update Fingerprint Features Request (A3310) message, which includes descriptive data, to AFIS/FBI. A3310 also contains the FILEHANDLE which AFIS/FBI uses to retrieve the image file from ITN/FBI. The image file is formatted in accordance with I3020. For an Ident, AFIS/FBI updates features if AFIS/FBI or a Service Provider determines them to be better than descriptive information in the Criminal Master File. For a criminal Non-Ident retain, AFIS/FBI creates a new record.

If the submission resulted in a Criminal Non-Ident Retain or in a Criminal Ident with upgraded features, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

(20) AFIS/FBI returns the Update Fingerprint Features Response (A3311) message which includes the pattern classification.

(21) ITN/FBI sends III/FBI the File Maintenance Completion Notification (A3331), which includes the pattern classification and ten-print certification pointer. III/FBI does not respond to this message.

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3401 Hit to Want Notification
N3102 No Prior Record – Civil (CFN)
N3103 Prior Record – Civil (CFR0029
N3107 Unsolicited Deceased Notification
N3112 (MSO) Multi-state Offender Status
N3114 (NMS) Non-matching SID Ignored
N3115 (NPR) No Prior Record—SID Entered
N3116 (PES) Prior Record—Previously Entered SID Notification (Single)
N3117 (PIR) Prior Record—SID Entered
N3119 (RNP) Reject, No Prior Record, SID Not Entered
N3120 (RPR) Reject, Prior Record, SID Not Entered
N3123 Prior Record- Previously Entered SID (multi)
N3126 SOR Agency Notice

Figure 21.1-02b Electronically submitted, Internally Processed Ten-Print Submission Data Flow Sequencing and Notes

This diagram applies to the following STOTs: FNDR, NNDR, and CPDR. This diagram illustrates IAFIS processing of externally submitted, internally processed ten-print submissions Federal No-Charge Direct Route (FNDR), Non-Federal No-Charge Direct Route (NNDR), and Criminal Print Direct Route (CPDR). CPDR is a Criminal STOT while FNDR and NNDR are Civil STOTs. If the submission results in an Ident, the submission data is used to update the existing records in the Criminal Files. If the submission results in a Non-Ident and the submission is to be retained, the submission data is used to create a new record in the Criminal files. The Files used in the process include: 1) the Criminal Ten-Print Fingerprint Image Master File (FIMF) (ITN/FBI), 2) the Ten-Print Certification File (TPCF) (ITN/FBI), 3) the Unsolved Latent Fingerprint Image File (ULF) (ITN/FBI), 4) the Subject Criminal History File (SCH) (III/FBI), and 5) the Criminal Ten-Print Features Master File (CMF) (AFIS/FBI).

(1) IAFIS receives the EBTS Ten-Print Submission (E1000) message via the CJIS WAN.

(2) At Automated Quality Check, the submission STOT and Type of Search Requested (TSR) value is checked and, if the STOT is FNDR, NNDR, or CPDR and the TSR is 'C,' the submission is placed on the Special Stops Log to be reviewed by a Special Stops Service Provider. The Special Stops Service Provider will request a subject search causing ITN/FBI to send the Subject Search Request (A1030) message to III/FBI and, optionally, will include the supplied FNU.

(3) If a supplied FNU has been killed as the result of a previous consolidation and the kept FNU was not returned as a candidate from the subject search, III/FBI will include the associated kept FNU in the Ten-Print Subject Search Response (A1031) message. This subject search is performed against the SCH File which produces a list of FBI Numbers (candidate list). The subject of a supplied FNU will also be returned as a candidate. III/FBI will perform filtering. For ITN/FBI handling of special subjects (Wants AUD values), refer to IAFIS System Design Document (ISDD), Design Note #17.

(4) If filtering reveals a subject record containing AUD = 'T' and an SPF= 'T,' ITN/FBI will route the transaction to Answer Hits to Wants. In these instances, ITN/FBI will pre-stage the desired criminal histories using the A1032/A1033 message pair.

ITN will attempt to retrieve images for any candidates returned in the A1031 message. These candidate images will be compared against the submission images, and identification decisions will be made by the Special Stops Service Provider.

(5) If a Non-Ident has resulted from the preceding subject search, the Special Stops Service Provider will request a Ten-Print Features Search, causing ITN/FBI to send the AFIS Ten-print Search (A1027) message to AFIS/FBI to initiate a search of the Criminal Ten-print Features Master File (CMF). The A1027 contains the FILEHANDLE which AFIS/FBI will use to retrieve the file containing images from ITN/FBI. The file is formatted in accordance with I3020.

(6) AFIS/FBI will respond with the AFIS Search Response Data Candidate List (A1022) message.

ITN will attempt to retrieve images for any candidates returned in the A1022 message. These candidate images will be compared against the submission images and identification decisions will be made by the Special Stops Service Provider.

NOTE: If the submission resulted in multiple criminal Idents, the Special Stops Service Provider completes Consolidation processing. This consolidation process is described in Figure 21.3-02 and then returns to this DFD.

(7) Upon completion of all necessary searches, the Special Stops Service Provider will request that a response be generated. This request causes ITN/FBI to send the Ten-Print Criminal History File Maintenance Request (A3026) message to III/FBI for submissions Idented against the criminal files or for Criminal Non-Ident Retains.

If filtering reveals a SPF = 'K,' and the transaction has not been reviewed by DOC SPEC, III/FBI will reject the A3026 for Unauthorized Access with an A1802. When this rejection occurs, ITN/FBI will route the transaction to DOC SPEC for review. Upon completion of the review, ITN/FBI will resend A3026.

The following subset of message flows applies to completing the submission response.

*****III/FBI generates and sends a QTP Request Message to NCIC following the start of File Maintenance and after the completion of any required manual reviews.**

(8) If the subject record (from an Idented submission) contains active NFF state pointers, III/FBI will send an N3105 message via NCIC to any states that have a criminal history on the subject.

(9) III/FBI will queue the FBI portion of the response until the state criminal history data is returned in the Nlets CR Response (L1048) message. III/FBI will code the A1003 with an electronic rap sheet (ERS) containing the FBI-held portion of the record together with the criminal history data received from the NFF states (L1048).

(10) If the A3026 attempted to update a record containing a Want and if the submission is civil, III/FBI suspends generation of the A1003 and sends the File Maintenance Response (A3025) message to ITN/FBI.

(11) If this occurs, III/FBI will generate a Review Request (A1312) message that will be routed to AHTW for review and processing. Civil hits to Wants result in Service Provider phone contact with the Want originator.

(12) The Service Provider may release the transaction for response generation after the review. The result of the AHTW review is a Review Response (A1313) message sent from ITN/FBI to III/FBI.

Note: If the submission is a civil, the A1313 may redirect III/FBI to send a Non-Deceased Fingerprint Card On-Line Hit Notification report via an Unsolicited Hit to Want Notification (N3401).

Note: If a criminal submission hits to a Want, the preceding Review Request and Response are omitted and III/FBI sends a Non-Deceased Fingerprint Card On-Line Hit Notification report via an Unsolicited Hit to Want Notification (N3401) to the Want Originator and the Arresting Agency.

NOTE: If A3026 updates a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) message to all registering agencies. III/FBI then proceeds to perform response generation.

(13) III/FBI provides responses to the submission: III/FBI will collect criminal history information from NFF states if necessary, then format the A1003 and send it to ITN/FBI. ITN/FBI will format the E1003 and will forward it to EFCON which will send the message to the contributor via the CJIS WAN.

(14) At the request of the Special Stops Service Provider, III/FBI may redirect the hardcopy response to ITN/FBI (ONC = 'R' or TOO = 'W') via an Unsolicited Report (A3150) message containing the IDRR/NIDR.

The following subset of message flows applies to completing the file maintenance process.

(15) III/FBI responds to the A3026 of the Ten-Print File Maintenance Response (A3025), triggering the ITN/FBI update to the Fingerprint Image Master File and to start the update with AFIS/FBI. A3025 also triggers the update of the Ten Print Certification File for additions or updates to the criminal files.

(16) ITN/FBI sends an Update Fingerprint Features Request (A3310) message, which includes descriptive data, to AFIS/FBI. A3310 also contains the FILEHANDLE which AFIS/FBI uses to retrieve the image file from ITN/FBI. The image file is formatted in accordance with I3020.

(17) AFIS/FBI returns the Update Fingerprint Features Response (A3311) message which includes the pattern classification.

(18) ITN/FBI sends III/FBI the File Maintenance Completion Notification (A3331), which includes the pattern classification and ten-print certification pointer. III/FBI does not respond to this message.

NOTE: If the submission resulted in AFIS/FBI upgrading its features, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3401 Hit to Want Notification
N3102 (CFN) No Prior Record—Civil
N3103 (CFR) Prior Record—Civil
N3107 Unsolicited Deceased Notification
N3112 (MSO) Multi-state Offender Status
N3114 (NMS) Non-matching SID Ignored
N3115 (NPR) No Prior Record—SID Entered
N3116 (PES) Prior Record—Previously Entered SID Notification (Single)
N3117 (PIR) Prior Record—SID Entered
N3119 (RNP) Reject, No Prior Record, SID Not Entered
N3120 (RPR) Reject, Prior Record, SID Not Entered

Figure 21.1-03 Remote Ten-print Search Data Flow Sequencing and Notes

This DFD applies to the STOTs TPFS and TPIS. This diagram illustrates IAFIS processing of an electronic Ten-print search initiated by a remote user. This search results in the return of a list of candidates for evaluation by the remote user—an Ident/Non-Ident decision is NOT a part of this process.

(1) IAFIS receives the EBTS Ten-print Fingerprint Search (E1020) message from a remote user via the CJIS WAN. ITN/FBI prepares the Remote Ten-print Fingerprint Search (A1020) message, containing the FILEHANDLE, and the E1020 Message File Format (I1020). The FILEHANDLE element is the location of the I1020 file. The A1020 message is sent to AFIS/FBI.

(2) AFIS/FBI will perform the requested search and sends the Remote Ten-print Search Candidate List (A1006) message to III/FBI.

(3) If no candidates are sent in the A1006, then III/FBI will continue with paragraph 7; otherwise, III/FBI performs filtering on the list of candidates. If any of the candidate records contain flags or codes indicating that the record requires special attention, III/FBI will send a Review Request (A1312) message to ITN/FBI that will be routed to a Special Stops Service Provider for review and processing.

(4) The result of the Special Stops Service Provider review is returned in the Review Response (A1313) message sent from ITN/FBI to III/FBI.

(5) III/FBI will send the Internal Ten-print Image Request (A1057) message to ITN/FBI requesting that the images for the top candidate whose record contains an AUD = 'BLANK' and is produced as a result of the search be retrieved.

(6) ITN/FBI will respond to III/FBI with the Internal Ten-print Image Response (A1058) message containing the FNU of the top candidate indicating that the requested images have been retrieved for inclusion in the EBTS response.

(7) III/FBI will format the Search Response Candidate List (A1023) message and send it to ITN/FBI. ITN/FBI will convert the message and append all necessary images to the Search Results Ten-print (SRT) (E1023) message. ITN/FBI will send the E1023 to EFCON which will send the message to the contributor via the CJIS WAN.

Figure 21.1-04 Sexual Offender Registry (SOR) Data Flow Sequencing and Notes

This diagram illustrates IAFIS processing of Sexual Offender Registry (SOR) transactions sent by NCIC to IAFIS.

(1) NCIC sends Enter, Modify, Clear, or Cancel transactions in the $.A.WPT (N1810) message directly to III/FBI. III/FBI will automatically post the SOR data if it passes III/FBI edits and is accepted.

(2) III/FBI performs filtering; if III/FBI detects a Special Stop subject containing an SPF of '5,' III/FBI will send an Unsolicited Report (A3150) message to ITN/FBI, and will send an Unsolicited Activity Report (N3124) message to NCIC. If III/FBI detects a Special Stop subject containing an SPF of '6,' 'C,' or 'N,' III/FBI will send an Unsolicited Report (A3150) message to ITN/FBI to be generated in the Special Stops Unit. If III/FBI detects a special documentation subject containing an SPF K or DOD, III/FBI will send an Unsolicited Report (A3150) message to ITN/FBI to be generated in the DOC SPEC Unit. If no Special Stop subject was detected, but III/FBI detects a Wanted subject (SPF = 'L'), III/FBI will send the appropriate Hit to Want (N3401) message to the owner of the Want. If the subject record contains a SPF = 'I' or 'T', III/FBI will send an Unsolicited Report (A3150) message to ITN/FBI for routing to the Wants group.

(3) SOR transactions will be rejected if discrepancies exist between the incoming SOR data and IAFIS's stored data for the quoted FNU. When this occurs, an SOR Reject Notice will be sent to ITN/FBI by III/FBI via an Unsolicited Report (A3150) message to be printed on the Answer Hits to SOR printer. When SOR data is entered into the record of a subject containing manual arrest records (AUD = 'M'), III/FBI will send an SOR Reject Notice via an Unsolicited Report (A3150) message to ITN/FBI to be printed on the Answer Hits to SOR printer. This notice will serve as an alert to the DPS Service Provider that conversion of the subject manual arrest record is required.

The following is a list of unsolicited reports that may be spawned and sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
III Participant Online Printer Response—Hit Against SPF 5, 6, C, N, K or DOD	Special Stops DOC SPEC
SOR Reject Notice	Answer Hits to SOR
III Participant Online Printer Response—Hit Against Missing Person, Amnesia Victim or Wanted Subject Report	Answer Hits to Wants

The following is a list of messages which may spawn from processing an SOR transaction. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3401 Hit to Want Notification
N3112 (MSO) Multi-state Offender Status
N3121 (SSO) Single State Offender Status Notification
N3124 Unsolicited Activity Notification

Figure 21.1-05 Want Notification Data Flow Sequencing and Notes

This DFD applies to the STOTs WPT and WPTD. A Want enters IAFIS in one of two ways: (1) those with an assigned FNU will be sent electronically from NCIC to IAFIS and assigned the STOT WPT, or (2) hardcopy notification that will be entered manually by an IAFIS document processing Service Provider and assigned the STOT WPTD. A Want Notification may come in electronically from NCIC as an Enter Want (MKE EW or EW-C), Modify Want (MKE MW), Locate Want (MKE LW), Clear Want (MKE CW), or Cancel Want (MKE XW). This data flow shows how a Want Notification is processed by IAFIS.

(1) Electronic (STOT WPT): If the Want has an associated FNU or an NCIC Want Notification, $.A.WPT, an (N1810) message will be sent by NCIC directly to III/FBI. III/FBI will automatically post the Want if it is accepted.

(2) Document (STOT WPTD): The service provider searches for the subject and retrieves the record for review and verification. ITN/FBI sends a Service Provider Subject Search Request (A1032) message to III/FBI which contains an FBI number.

(3) Electronic (STOT WPT): A Want will be rejected if discrepancies exist between the incoming Want data and IAFIS's stored data for the quoted FNU. When this occurs, an Unsolicited Report (A3150) message containing either an NCIC Reject Response (NCIC Want Posting) or NCIC Reject Response (NCIC Want modifications and cancellations) will be sent by III/FBI to ITN/FBI to print on the Answer Hits to Wants printer. III/FBI performs filtering; if III/FBI detects any Special Stops subjects, III/FBI will abort processing and send an Unsolicited Report (A3150) message to ITN to be printed on the Special Stops Unit Printer.

(4) Document only (STOT WPTD): An A1032 containing an FNU is sent to III/FBI which returns a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

(5)After determining the record is the one of interest, if the service provider requests a printout, ITN/FBI will send a Criminal History Request (A1040) message to III/FBI and

(6) ITN/FBI will receive a Criminal History Request Response (A1042) message from III/FBI for printing (Refer to DFD 21.4-02).

Want Notifications that cannot be matched to an SCH record will be rejected except as described in (3).

(7) Document only (STOT WPTD): For want posting (EW or EW-C, Enter Want), the Want Service Provider will initiate a Want Notification (A1811) message. For Bureau Fugitives that are received with no FBI number and cannot be positively identified as a current SCH file record, the Wants Service Provider will create an AUD='T' record. Local and state Wants are posted if the reason for the initial reject has been resolved. For LW (Locate Want), CW (Clear Want), and XW (Cancel Want), the A1811 message will also be used.

(8) For MW (Modify Want), a SCH Modification will be used (A3038) (see DFD 21.3-13). For CW or XW, if the last or only Want being canceled is contained in a record with AUD='P,' the record will be deleted. If the record is to remain following removal of the last Want, SCH Modification should be used to remove the Want.

If filtering reveals a Special Stop subject and if the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A1811 or A3038 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A1811 or A3038, as appropriate for the transaction.

(9) Document only (STOT WPTD): III/FBI will return the File Maintenance Response (A3027) message to ITN/FBI.

(10) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI if the modification changes the subject descriptive data.

(11) If ITN/FBI receives A3045, it sends an Update Descriptive Data Request (A3312) message to AFIS/FBI.

(12) If a subject record contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(13) The state data is returned in the Nlets CR Response (L1048) message.

(14) III/FBI provides a hardcopy criminal history record report to agencies associated with the subject.

(15) Document only (STOT WPTD): If a Service Desk provider or Special Stops provider is processing the action, III/FBI may generate an Unsolicited Report (A3150) message in addition to or instead of printing a hardcopy report on the III/FBI high-speed printer:

Report Title	Destination Printer
MF Identification Response	Answer Hits to Wants
SCH Response	Answer Hits to Wants
NCIC Reject Response (NCIC Want posting)	Answer Hits to Wants, or Special Stops Unit (for SPF = '5' or '6' or 'C' or 'N')
NCIC Reject Response (NCIC Want modifications and cancellations)	Answer Hits to Wants, or Special Stops Unit (for SPF = '5' or '6' or "C' or 'N')
IDRR/NIDR	Special Stops Unit
IDRR/NIDR	Service Desk

The following is a list of messages which may be spawned when posting a Want. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3112 (MSO) Multi-state Offender Status
N3121 (SSO) Single State Offender Status Notification
N3124 Unsolicited Activity Notification

Figure 21.1-06 Flash Notification Data Flow Sequencing and Notes

This DFD applies to the STOT FLASH. This diagram illustrates IAFIS processing of a Flash Notification. A Flash will not be entered in IAFIS electronically; these notices will be entered manually by an ITN/FBI Document Processing Service Provider.

(1) A Service Provider will enter Flash information by first entering the FNU and submitting the A1032 request to III/FBI for review of the Subject Candidate Record.

(2) III/FBI will return the A1033.

(3) Once the Service Provider has reviewed the record set, they will submit the Flash notification via an ITN/FBI Workstation. ITN/FBI will forward the information to III/FBI in the Flash Notification (A1812) message.

III/FBI will process the Flash. A Flash will be rejected if discrepancies exist between the Flash data and the IAFIS-stored criminal history record or if no criminal history record is found for the Flash, either because it was never entered into IAFIS or because it was kept by an NFF state.

When this occurs, an Error Message (A1802) will be forwarded by III/FBI to ITN/FBI.

If a Flash is rejected because filtering reveals a special stop subject, and the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A1812 for Unauthorized Access. When this rejection for Unauthorized Access occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A1812.

(4) When the Flash is successfully posted, III/FBI returns the File Maintenance Response (A3027) message to ITN/FBI.

(5) Upon completion of file maintenance when posting a Flash to a record with a Want, III/FBI will send a Review Request (A1312) message that will be routed to AHTW for review and processing.

(6) The Service Provider may release the transaction for response generation after the review. The result of the AHTW review is a Review Response (A1313) message sent from ITN/FBI to III/FBI. If needed, the Service Provider may use an SCH Modification (see DFD 21.3-13) to remove the Want information prior to initiating the A1313 for transaction completion.

(7) If a subject record contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(8) The state data is returned in the Nlets CR Response/State Criminal History Data (L1048) message.

(9) III/FBI provides a hardcopy criminal history record report to agencies associated with the subject.

(10) If a Service Desk provider or Special Stops provider is processing the action, III/FBI may generate an Unsolicited Report (A3150) message in addition to or instead of printing a hardcopy report on the III/FBI high-speed printer:

Report	Destination Printer
IDRR/NIDR	Special Stops Unit

IDRR/NIDR	Service Desk

Figure 21.1-07 Civil Record Data Retrieval Sequencing and Notes

The diagram applies to the STOT CRDR, and illustrates the messaging sequence used when a Service Provider requests a Civil Record Set from III/FBI.

This flow represents the interaction between the Service Provider and IAFIS. The Service Provider makes the request and may receive a displayed response on the workstation.

(1) At the request of an ITN/FBI Document Processing Service Provider, ITN/FBI will send a Civil Subject Data Request (A1043) to III/FBI.

(2) III/FBI will respond with the Civil Subject Data Response (A1044) message. The contents of the A1044 message will be displayed at the ITN/FBI workstation.

Figure 21.1-08 Ten-Print-Initiated Search of Unsolved Latent File Data Flow Sequencing and Notes

This DFD applies to the STOT ULM. This diagram illustrates IAFIS processing of the Unsolved Latent File search. This search takes place whenever AFIS/FBI receives a features update request (A3310 message) under any of the following circumstances:

- new record add (AAC = '1') to the Criminal Master File (CMF);
- AFIS/FBI produces significantly better features (AAC = '2') as a result of an update to an existing record in the CMF; or
- forced update (AAC = '4') to an existing record in the CMF.

The ULF searches are spawned from any ten-print submission which performs file maintenance. This data flow has been separated from the other diagrams for the sake of clarity.

The Unsolved Latent Features File contains saved latent searches, each of which may contain the features of more than one finger. Each saved search is identified by the AFIS segment control number (SCNA). **If multiple ULF candidate matches are made from the features of the same saved multi-finger latent search (the SCNA is the same for each candidate match), the flows below occur once. If AFIS/FBI produces multiple ULF candidate matches to different searches (different SCNAs), the flows below occur once for each saved latent search (each SCNA) from which AFIS/FBI made a match.**

(1) If the initiating submission resulted in one of the three conditions described in the first paragraph, AFIS/FBI initiates a search of the Unsolved Latent File. If no candidates are found, none of the following steps will occur. One Response Data Unsolved Latent Match (A1004) message will be sent to III/FBI for each saved latent search (each SCNA) from which AFIS/FBI made a match. III/FBI will filter all Unsolved Latent Match Responses.

(2) If filtering of SCH reveals a Special Stop subject, III/FBI sends a Review Request (A1312) message to ITN/FBI for routing to the Special Stops Unit. Note that this is required even though the initiating Ten-Print Submission was reviewed.

(3) Following the review, ITN/FBI returns the Review Response (A1313).

(4) If the owner of the unsolved latent fingerprint is not FAS, III/FBI sends the Unsolved Latent Fingerprint Image Request (A1055) message to ITN/FBI to prepare the image of the ten-print candidate finger and, if available, of the unsolved latent record for return to the submitter (some unsolved latent records will not have associated images).

(5) ITN/FBI returns the Unsolved Latent Fingerprint Image Response (A1056) message when image retrieval completes.

(6) For externally-owned latent fingerprints, III/FBI produces the Unsolved Latent Match (External) (A1005) message in EBTS format and sends it to ITN/FBI. ITN/FBI will convert the message to the External Unsolved Latent Candidate Match (E1005). ITN/FBI will append the retrieved image(s) when preparing the E1005. ITN/FBI will send the E1005 to EFCON which will send the message to the contributor via the CJIS WAN.

(7) For latent fingerprints owned internally, III/FBI sends the Unsolved Latent Match (Internal) (A1007) message to ITN/FBI for routing to FAS with the retrieved image(s).

ITN/FBI will create an entry on the Assignment Log to be assigned to a Latent Examiner.

After the Latent Supervisor assigns a Latent Examiner to the ULM, ITN/FBI will create an entry on the Latent Examiner's Submission Log, and the submitted Ten Print images and the matched ULF image will be available on the Image Log

ITN/FBI will send an email to the Latent Examiner assigned to the ULM notifying of the new submission.

Figure 21.1-09 Civil Record Subject Search Data Flow Sequencing and Notes

The diagram applies to the STOT CRSS and illustrates IAFIS processing of the Civil Record Subject Search. These requests are typically issued by either an ITN Service provider, a Latent Specialist, or a NICS Examiner. This flow represents the interaction of ITN/FBI with the Service Provider and III/FBI with the NICS examiner.

A Service Provider or a NICS Examiner at an ITN Workstation submits the search request.

(1) ITN/FBI or NICS sends a Civil Subject Retrieval Request (A1061) message to III/FBI which will contain a CRN number or descriptive data. III/FBI will retrieve the subject record if an active CRN number is provided in the request otherwise III/FBI will perform a civil subject search.

(2) If a single CRN is to be provided, III/FBI returns a Civil Candidate Record (A1060) message which contains the criminal history data for that subject. If no CRN is provided and the civil subject search returns only one candidate, III/FBI will return that candidate record in the A1060.

(3) If the CRN provided is not correct, III/FBI will return a Civil Candidate List (A1059) with no candidates. At this point the Service Provider can either re-issue the A1061 message with the correct CRN number or reject the process. If no CRN is provided but descriptive data is provided, III/FBI will perform a civil subject search and return possible candidates in the A1059.

Figure 21.1-10 ULF Search Enhancement Data Flow Sequencing and Notes

This DFD applies to the STOT ULM. This diagram illustrates IAFIS processing of the Unsolved Latent File search. The search takes place whenever a Criminal or Humanitarian submission is non-retain (RET = N) and results in a non-identification decision. This dataflow has been separated from the other diagrams for the sake of clarity.

The Unsolved Latent Features File contains saved latent searches, each of which may contain the features of more than one finger. Each saved search is identified by the AFIS/FBI segment control number (SCNA). **If multiple ULF candidate matches are made from the features of the same saved multi-finger latent search (the SCNA is the same for each candidate match), the flows below occur once. If AFIS/FBI produces multiple ULF candidate matches to different searches (different SCNAs), the flows below occur once for each saved latent search (each SCNA) from which AFIS/FBI made a match.**

(1) When a criminal Ten-Print or Humanitarian Return submission has completed with a Non-Identification decision, ITN/FBI will send a Directed ULF Ten-Print Search (A1018) to AFIS/FBI.

(2) When the search completes, AFIS/FBI will return an A1019 message to ITN/FBI.

If no candidates are returned in the A1019, then ITN/FBI will clean up the submission, and processing is complete.

If candidates are returned, ITN/FBI will create a new UCN for the submitted TP images and use it to create a Cert File.

If candidates are returned, ITN/FBI will request the appropriate latent images (if available) and stage them in the LEFF for compare.

(3) For each candidate in the A1019 where the ULF owner is not a Latent Examiner, ITN/FBI will create the E1005 (ULM) message: which will include the UCN, biographic data, 10 rolled TP images, and the ULF image (if available): and send it to EFCON. EFCON will send the E1005 message to the remote ULF owner.

After the E1005 message has been successfully sent, ITN/FBI will clean up, and the submission will be complete.

For each candidate in the A1019 where the ULF owner is a Latent Examiner, ITN/FBI will stage both the submitted Ten Print images and the matched ULF image for compare using the latent case number (LCN) from the A1019 message and the next available latent case extension (LCX).

ITN/FBI will send an email to the owners of the ULF record notifying them that a Cascaded ULF search hit their ULF record.

ITN/FBI will create an entry on the Assignment Log to be assigned to a Latent Examiner.

ITN/FBI will clean up the Ten Print submission.

After the Latent Supervisor assigns a Latent Examiner to the ULM, ITN/FBI will create an entry on the Latent Examiner's Submission Log, and the submitted Ten Print images and the matched ULF image will be available on the Image Log

ITN/FBI will send an email to the Latent Examiner assigned to the ULM notifying of the new submission.

Figure 21.2-01 External Fingerprint Image Submission Data Flow Sequencing and Notes

This diagram applies to the STOT FIS. This diagram illustrates IAFIS processing of the External Fingerprint Image Submission. Because it allows a user, typically an NFF state, to submit a better fingerprint image (or images) rather than just a request for identification, it is distinct from the ten-print submission.

(1) IAFIS receives the EBTS Fingerprint Image Submission (E1060) message via the CJIS WAN. This message contains the data set T4HIGRAY, a complete set of fourteen images, and a mandatory FNU.

(2) ITN retrieves images and a Ten-print Service Provider performs an image comparison confirming the identity of the subject and evaluating the worth of the new submission images as replacements. If the Service Provider Idents the submission, then ITN/FBI sends the Image Submission File Maintenance Request (A3000) message to III/FBI; otherwise, ITN/FBI rejects the submission with the EBTS Error Response Request (A1801) message to III/FBI. (Refer to DFD 21.6-01 for error processing detail.)

NOTE: If filtering reveals a Special Stop subject with an SPF of '5,' III/FBI sends an Unsolicited Activity Notification (N3124) message via NCIC network.

NOTE: If the subject record has a Want (SPF = L, I, or T), III/FBI sends a Hit to Want Notification (N3401) via NCIC network.

(3) The Fingerprint Image Response (A1062) message is sent from III/FBI to ITN/FBI. ITN/FBI will convert the message to an E1062 and send it to EFCON which will send the message to the contributor via the CJIS WAN. This message contains the finger number(s) of the image(s) updated.

(4) III/FBI sends the Ten-Print File Maintenance Response (A3025) message to ITN/FBI, initiating an update of the Fingerprint Image Master File. The Fingerprint Image Submission will result in an update to an image only if it is determined that the image is of higher quality than that currently in the FIMF.

(5) ITN/FBI sends the Update Fingerprint Features Request (A3310) message to AFIS/FBI to update its Criminal Master File, as appropriate. A3310 contains the FILEHANDLE which AFIS/FBI will use to retrieve the file containing images from ITN/FBI. The file is formatted in accordance with I3020.

(6) AFIS/FBI returns the Fingerprint Features Response (A3311) message, which includes the pattern classification.

(7) ITN/FBI sends the File Maintenance Completion Notification (A3331) message, with the current pattern classification, to III/FBI. This message does not include the Ten-print Certification File Index, because III/FBI does not maintain an arrest cycle for this type of submission. However, the index is maintained in the Transaction History Database in ITN/FBI.

AFIS/FBI initiates a search of the Unsolved Latent File by finger if features for any finger are replaced with those of a higher quality. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (DFD 21.1-08).

The following is a list of unsolicited messages that may be spawned from processing an External Fingerprint Image Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/ Name

N3124 Unsolicited Activity Notification
N3401 Hit to Want Notification

Figure 21.2-02 Internal Fingerprint Image Submission Data Flow Sequencing and Notes

This data flow applies to the STOT IFIS. This diagram illustrates IAFIS processing of the Internal Fingerprint Image Submission. Because it allows a user, typically an NFF state, to submit a better fingerprint image (or images) rather than as a request for identification, it is distinct from the ten-print submission. If the submissions result in an Ident, the submission data is used to update the existing records in the Criminal Files. If the submission results in a Non-Ident and the submission is to be retained, the submission data is used to create a new record in the Criminal files. The Files used in the process include: 1) the Criminal Ten-Print Fingerprint Image Master File (FIMF) (ITN/FBI), 2) the Ten-Print Certification File (TPCF) (ITN/FBI), 3) the Unsolved Latent Fingerprint Image File (ULF) (ITN/FBI), 4) the Subject Criminal History File (SCH) (III/FBI), and 5) the Criminal Ten-Print Features Master File (CMF) (AFIS/FBI).

An ITN/FBI Service Provider will scan the fingerprint card and perform the necessary data entry at a workstation

(1) The Service Provider performs an image comparison confirming the identity of the subject and evaluating the worth of the new submission images as replacements. If the Service Provider Idents the submission; then ITN/FBI sends the Image Submission File Maintenance Request (A3000) message to III/FBI; otherwise, ITN/FBI rejects the submission.

NOTE: If filtering reveals a Special Stop subject with an SPF of '5,' III/FBI sends an Unsolicited Activity Notification N3124) message via NCIC network (see Unsolicited Messages below).

NOTE: If the subject record has a Want (SPF = L, I, or T), III/FBI sends a Hit to Want Notification (N3401) via NCIC network. (See the list of Unsolicited Messages below.)

*****III/FBI generates and sends a QTP Request Message to NCIC following the start of File Maintenance and after the completion of any required manual reviews.**

(2) III/FBI sends the Ten-Print File Maintenance Response (A3025) message to ITN/FBI, initiating an update of the Fingerprint Image Master File. The Fingerprint Image Submission will result in an update to an image only if it is determined that the image is of higher quality than that currently in the FIMF. If no image update(s) occurred, flows 4, 5, and 6 will not occur.

(3) ITN/FBI sends the Update Fingerprint Features Request (A3310) message to AFIS/FBI requesting an update to its Criminal Master File, as appropriate. A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the image file from ITN/FBI. The file is formatted in accordance with I3020.

(4) AFIS/FBI returns the Fingerprint Features Response (A3311) message which includes the pattern classification.

(5) ITN/FBI sends the File Maintenance Completion Notification (A3331) message, including the pattern classification, to III/FBI. This message does not include the Ten-print Certification File Index, because III/FBI does not maintain an arrest cycle for this type of submission. However, the index is maintained in the Transaction History Database in ITN/FBI.

AFIS/FBI initiates a search of unsolved latent by finger if features for any finger are replaced with a higher quality image. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

The following is a list of unsolicited messages that may be spawned from processing an Internal Fingerprint Image Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

N3401 Hit to Want Notification

Message Number/ Name
N3124 Unsolicited Activity Notification

Figure 21.2-03 External Fingerprint Image Request Data Flow Sequencing and Notes

This DFD applies to the STOT IRQ. This diagram illustrates IAFIS processing of the EBTS IRQ (Image Request) transaction. An external user may request up to 1000 subject sets of fingerprint images, optionally indicating specific fingers. If the supplied FBI number has images, the requested finger(s) is returned. Each FBI number supplied in an initiating EBTS Fingerprint Image Request message with the requested images on file results in a separate EBTS Fingerprint Image Request Response message. An EBTS Image Summary Response message summarizing the status of the individual responses is sent upon completion of the process.

(1) The EBTS Fingerprint Image Request (E1050) message is received by IAFIS from an external user via the CJIS WAN. This request must include an FBI number(s). (The user can obtain the FBI number(s) prior to requesting images by submitting the corresponding SID(s) using the NCIC Criminal History Request or Subject Search processes.)

(2) ITN/FBI sends the Filter Request (A1310) message with the received list of up to 1000 FNUs to III/FBI.

(3) III/FBI returns the list of FNUs in the Filter Response (A1311) message. For each FNU, a) AUD is returned, if the FNU is in the SCH File, and b) SPF is returned, if appropriate (see message-level detail). If any FNU is the record identifier for a Special Stop subject, then the entire list is routed to the Special Stops Unit for review.

(4) ITN/FBI then retrieves images of the requested finger(s) or all fingers from FIMF for each FNU returned with AUD = 'Blank' and stages them to be appended to the response message. One Fingerprint Image Response Data (A1051) message is created for each FNU/image set and sent to III/FBI.

(5) Each A1051 message received by III/FBI initiates a separate Fingerprint Image Request Response (A1052) message for return to ITN/FBI. ITN/FBI then appends the staged image(s) to the E1052 and sends it to EFCON which will send the message to the contributor via the CJIS WAN.

(6) ITN/FBI creates a summary of the results of the image request, listing each of the FNUs only if images were returned. The resultant Image Summary Response (A1063) message is sent to III/FBI.

(7) III/FBI builds the Formatted Image Response Summary (A1064) message and sends it to ITN/FBI. ITN/FBI converts the message into an E1064 and sends the Image Response Summary (E1064) message to EFCON which will send the message to the contributor via the CJIS WAN.

Message Number/ Name

N3124 Unsolicited Activity Notification

Figure 21.2-04 Internal Fingerprint Image Request Data Flow Sequencing and Notes

This DFD applies to the STOT IIRQ. This diagram illustrates the process by which IAFIS personnel retrieve a fingerprint image from the FIMF held in ITN/FBI.

A Service Provider requests subject fingerprint image(s) by providing the FNU(s) and, optionally, finger number(s) for the desired image(s).

(1) If the requester is (not AUTH of 6 or 7), ITN/FBI sends the Filter Request (A1310) message to III/FBI where the subject FNU list is checked for the presence of SPF flags and AUD code "T."

(2) If the requester is a latent specialist or an OFO Latent User (AUTH of 6 or 7), to present limited subject information with each requested image, ITN/FBI pre-stages the information by sending a Service Provider Subject Search Request (A1032) message, including an FNU and with CAND-LIST-FLAG = Y, to III/FBI.

NOTE: If the requester is an OFO Latent User, as determined by AUTH code, III/FBI will include only subjects whose records contain an AUD value equal to either "BLANK" or "M."

(3) In response to an A1310, III/FBI will respond with a Filter Response (A1311) message. If A1311 indicates that any special stop subjects were detected, ITN/FBI will suspend the entire transaction and route it to the Special Stops Unit. ITN/FBI will notify these requesters to bring the document to the Special Stops Unit. After review, if ten-print images are available for the subject, ITN/FBI then retrieves image from the FIMF.

(4) In response to A1032, III/FBI returns a Service Provider Subject Search Candidate List (A1029) message to ITN/FBI. If an FNU is the identifier for a sensitive subject, then the transaction is routed to the Special Stops Unit. If the requester is an FBI/FAS latent specialist, ITN/FBI will route only the stopped subject to the Special Stops Unit. ITN/FBI will allow the FAS specialist to view the remaining requested FNUs and will inform the specialist that the image for the stopped FNU is unavailable. The latent specialist will call the Special Stops Unit to determine further processing of the stopped FNU. For OFO Latent Users, as determined by AUTH code, ITN/FBI will remove any special stop subject from the list and indicate the FNU is not on file or that images are not available.

(5) If desired, a hard copy of the image may be printed locally.

Figure 21.2-05 External Criminal Photo Image Request Data Flow Sequencing and Notes

This DFD applies to the STOT CPR. This diagram illustrates IAFIS processing of a user request for a subject photo image (mugshot) from the Interstate Photo System (IPS) file held in III/FBI.

(1) The Criminal Subject Photo Request (E1090) message is received by EFCON via the CJIS WAN. It is then sent to ITN/FBI, where ITN/FBI performs validation and sends the Criminal Subject Photo Request (A1090) message to III/FBI for image retrieval. Up to four photos may be associated with each arrest for a subject. This request specifies the desired subject photo(s) by providing the FNU and, optionally, DOA or DOA/DOS, thus requesting either the most recent photo set or the photo set associated with the particular arrest cycle. A single photo from an arrest cycle photo set may not be requested separately from the remainder of the set. A1090 contains the element FILEHANDLE which contains the location specified by ITN/FBI to which III/FBI is to write the file containing the requested photos.

III/FBI performs filtering on the subject FNU. If filtering reveals

(2) a Special Stops Subject (SPF = '5' or '6' or 'C' or 'N"), III/FBI will suspend processing and send a Review Request (A1312) message to ITN/FBI

or;

(3) a wanted subject (SPF = 'I,' 'L,' or 'T'), or subject requiring Doc Spec authorization (SPF = 'K,' '1,' '2,' '3,' '4,' '7,' '8,' or '9'), or a record containing an AUD = 'T' or a DOD, III/FBI will process the request and send the Unsolicited Report (A3150) message to ITN/FBI to be routed to the appropriate printer.

NOTE: If the request is made against a record containing no photo, an error will be returned indicating that no photo is available.

The following is a list of reports that may be spawned when processing an External Criminal Photo Image Request; these reports will be formatted by III/FBI.

Report Title	Destination Printer
EBTS or Internal Online Printer Response—Hit Against 5, 6, C, K, N, DOD, Missing Person, Unknown Deceased, Amnesia Victim or Wanted Subject	Answer Hits to Wants (SPF = 'I,' 'L' or 'T' or an AUD = 'T' with SPF = 'T' but no SPF = '5,' '6,' 'C,' or 'N')
	Document Specialist (contains DOD or has SPF = 'K,' '1,' '2,' '3,' '4,' '7,' '8,' or '9')
	Special Stops (AUD = 'T' with SPF = '5,' 'C,' or 'N' but not SPF = T)

NOTE: Validation errors encountered by III/FBI in the A1090 message body will not result in an A1802 to ITN/FBI but will be rejected by III/FBI via A1804 to ITN/FBI. ITN/FBI converts the message to an E1804 and sends the E1804 to EFCON which will send it to the contributor via CJIS WAN. (Refer to DFD 21.6-01 for error processing detail.)

(4) Upon completion of review by the Special Stops Unit, ITN/FBI returns the Review Response (A1313) message to III/FBI.

(5) If the FNU is provided without a DOA or DOA/DOS and more than one photo or set of photos is on file for the subject, III/FBI retrieves the most recently submitted photo set, based on the DOA, stored in the subject record. If either a DOA or DOA/DOS are provided, the appropriate photos are retrieved. If no photos are associated with the supplied DOA or DOA/DOS, III/FBI will

retrieve the most recently submitted photo set based on the DOA stored in the subject record. The E1091 message will be created as an I1002 format file containing the retrieved photos and written to the location in ITN/FBI specified in the element FILEHANDLE received in A1090. III/FBI formats the response and sends the Criminal Photo Request Response (A1091) message to ITN/FBI. ITN/FBI will convert the message to a Criminal Photo Request Response (E1091) and sends the E1091 to EFCON which will send the message to the contributor via the CJIS WAN.

(6) If a no photos exist for FNU, III/FBI will use the A1804 error message carrying EBTS error. ITN/FBI will convert the message to an E1804 and send to the EFCON which will send the message to the contributor via the CJIS WAN. (Refer to DFD 21.6-01 for error processing detail.)

The following is a list of unsolicited messages which may be spawned from processing an external criminal photo image request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 21.2-07 External Criminal Photo Delete Request Data Flow Sequencing and Notes

This DFD applies to the STOT CPD. This diagram illustrates IAFIS processing of a user request for the deletion of a set of photos from the Interstate Photo System (IPS) File held in III/FBI. Only the owner (original submitter) may request the removal of a set of photos from the IPS. No unsolicited notification messages are sent via NCIC as a result of this transaction.

(1) ITN/FBI receives a Criminal Subject Photo Delete Request (E1092) message from an external user via EFCON, which receives the E1092 from the CJIS WAN. ITN/FBI performs validation and passes the Criminal Subject Photo Delete Request (A1092) message to III/FBI.

(2) III/FBI performs the requested delete using the provided FNU, DOA, and DOS and returns to ITN/FBI the Criminal Subject Photo Delete Response (A1093) message containing the FNU, DOA, and DOS with REC = 'Y.' If the requested deletion cannot be performed, III/FBI will send a reject using the E1804 error message carrying EBTS error set ERRI to ITN/FBI. ITN/FBI converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to the contributor via CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.). Otherwise, ITN/FBI receives the A1093 message and prepares the Criminal Subject Photo Delete Response (E1093) message which is sent to EFCON which forwards the message to the contributor via the CJIS WAN.

(3) After processing the delete request III/FBI performs filtering on the subject FNU. If filtering reveals a Special Stops (AUD = 'T' or SPF = '5,' 'C,' or 'N'), wanted subject (SPF = 'I,' 'L' or 'T'), or subject requiring Doc Spec authorization (SPF = 'K,' '1,' '2,' '3,' '4,' '7,' '8,' or '9' or an AUD not equal to N and a DOD), III/FBI will send the Unsolicited Report (A3150) message to ITN/FBI to be routed to the appropriate printer.

The following is a list of reports that may be spawned when processing an External Criminal Photo Image Delete Request; these reports will be formatted by III and printed by ITN/FBI.

Report Title	Destination Printer
EBTS or Internal Online Printer Response—Hit Against 5, 6, C, K, N, DOD, Missing Person, Unknown Deceased, Amnesia Victim or Wanted Subject	Answer Hits to Wants (SPF = 'I,' 'L' or 'T' or an AUD = 'T' with an SPF = 'T' but no SPF = '5,' '6,' 'C,' or 'N')
	Document Specialist (contains DOD or has SPF = 'K,' '1,' '2,' '3,' '4,' '7,' '8,' or '9')
	Special Stops (AUD = 'T' or SPF = '5,' 'C,' or 'N')

NOTE: Validation errors encountered by III/FBI in the A1092 message body will not result in an A1802 to ITN/FBI but will be rejected to the submitter by III/FBI sending an A1804 to ITN/FBI. ITN/FBI will convert the message to an E1804 and send it to EFCON which will send the message to the contributor via the CJIS WAN. (Refer to DFD 21.6-01 for error processing detail.)

Figure 21.3-02 Internal Consolidation Request Data Flow Sequencing and Notes

This DFD applies to the STOT COND. This data flow illustrates IAFIS processing of a request for consolidation of subject records when multiple records (multiple FNUs) are found to be held for a single subject. It corresponds to the case where the consolidation is associated with a ten-print submission as well as when the consolidation is initiated by a document. Consolidations only occur for criminal subjects, never for civil subjects.

Begin Document Consolidation

This flow represents the interaction of Service Providers as the consolidation activity occurs. The DPS Service Provider initiates the document-based consolidation by forwarding the FNU List to Ten Print processing.

Begin Ten-print Consolidation

(1) Images of the FNUs identified for the consolidation are retrieved and the AFIS Ten-Print Verify and Search (A1227) message is created with candidates. AFIS/FBI performs FNU III/Verify and prepares the AFIS FIC indicators.

(2) AFIS/FBI sends ITN/FBI the AFIS Ten-Print Verify and Search Response Data Candidate List (A1222). Follow External Criminal Ten-Print Submission Data Flow (21.1-01a) sequence 7 beginning with paragraph 2 for Fingerprint Image Comparison (FIC).

A consolidation spawned by the ten-print process begins here. In the case of a ten-print submission where multiple Idents occur, ITN/FBI routes the multiple candidates and submission to the evaluation unit.

The evaluation unit confirms that the images belong to the same subject.

(3) If the image comparison of the FNUs confirms a single subject, ITN/FBI initiates a Filter Request (A1310) message to III/FBI containing the FNUs being considered for consolidation.

(4) III/FBI will filter the provided list of FNUs and return the results in the Filter Response (A1311) message. If the list contains the FNU of a Special Stops Subject, the submission is routed to an authorized Service Provider which will complete consolidation processing. Otherwise, a DPS Service Provider completes the process. In either case, the following steps apply.

(5) Auto Consolidation: ITN/FBI will send a Consolidation File Maintenance Request (A3028) to III/FBI. III/FBI will apply business rules for the consolidation of the FNUs in the message. If the consolidation can not be completed, III/FBI returns Consolidation Response (A3082) with the auto-consolidation flag set to N and processing continues with paragraph 7. If the consolidation can be performed, then III/FBI returns the A3082 with the auto-consolidation flag set to Y with the 'kept FNU.' Processing continues with paragraph 10 except III/FBI will not return the A3027.

(6) Manual Consolidation: To determine which one of the multiple FNUs assigned to the subject should be retained; the Service Provider needs to review the Record Set of each of the FNUs involved in the consolidation. ITN/FBI sends Service Provider Subject Search Request (A1032) messages to request records using the FNUs identified for consolidation. A separate A1032 is initiated for each combination FNU/Record Set needed.

(7) For each A1032 request received, III/FBI will return a separate Service Provider Subject Search Candidate Record (A1033) message.

(8) If the A1032 requested a printed response, III/FBI will also send an Unsolicited Report (A3150) message to ITN/FBI. After review of the subject records, the Service Provider selects the FNU to keep.

(9) The Consolidation File Maintenance Request (A3028) message contains the FBI number of the subject to be kept and the FBI numbers (killed) of the subject records to be consolidated into the kept subject record. If filtering reveals a Special Stop subject and the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A3028 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3028.

(10) III/FBI performs the consolidation, if able to do so; III/FBI returns a File Maintenance Response (A3027) message to ITN/FBI. The A3027 may contain the element MSGCOD which is used to indicate that file maintenance was completed with a warning (see Error Code Table). If the consolidation is associated with a ten-print submission, ITN/FBI will allow file maintenance processing of the ten-print submission to resume at this point.

(11) If the A3028 attempted to update a record with a Bureau Fugitive Want after file maintenance, III/FBI then generates a Review Request (A1312) message that will be routed to a DPS Service Provider for review and processing.

(12) The Service Provider releases the transaction for response generation after the review and any necessary modifications by sending the Review Response (A1313) message to III/FBI.

(13) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI. For both types of consolidations (DPS or TPS initiated), the FIMF records for the "killed" FNUs are marked Inactive.

NOTE: If A3028 updates a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Records Consolidated Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) to all registering agencies and an SOR Hit Notice to the Answer Hits to SOR printer in an Unsolicited Report (A3150) message. III/FBI then proceeds to perform response generation.

(14) ITN/FBI sends an Update Fingerprint Features Request (A3310) message to AFIS/FBI to initiate an update of the features and descriptive data of the kept subject. ITN/FBI then applies the ten-print submission data to the CERT. The A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI. The image file is formatted in accordance with I3020, Type-4 Record Image File Format.

(15) AFIS/FBI returns an Update Fingerprint Features Response (A3311) message, which includes the pattern classification of the kept FNU, to ITN/FBI.

NOTE: In a consolidation associated with a ten-print submission, the image set for the kept FNU is sent to the FIMF and AFIS/FBI during the File Maintenance processing of the original ten-print submission. The A3310 contains the consolidated descriptive data and the image set for the kept FNU that were derived from the Idented records and the initiating ten-print submission. A3310 also contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI. The image file is formatted in accordance with I3020.

(16) In both types of consolidations for each "killed" FNU, ITN/FBI sends a Delete Fingerprint Features Request (A3321) message to AFIS/FBI.

(17) ITN/FBI sends a File Maintenance Completion Notification (A3331) message, which contains the new pattern level classification data for the kept subject and the CERT Index.

(18) If a subject record (in an Idented submission) contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(19) The state data is returned in the Nlets CR Response (L1048) message. (Does not apply if the consolidation is associated with a ten-print submission)

(20) III/FBI provides a hardcopy criminal history record report to agencies associated with the subject. This will only occur when the consolidation is not associated with a ten-print submission. For a consolidation associated with a ten-print submission, the response will be sent during the File Maintenance Request processing of the origional ten-print submission, and will include an indication that the subject records have been consolidated. In consolidation cases, document- or ten-print-initiated, III/FBI will query the CRS file for the kept FNU and sends a copy of the response to each contributor listed for the previous twelve-month period.

If a Service Desk provider or Special Stops provider has initiated the action, III/FBI may generate an Unsolicited Report (A3150) message in addition to or instead of printing a hardcopy report on the ITN/FBI printer:

Report Title	Destination Printer
IDRR/NIDR	Special Stops Unit
IDRR/NIDR	Service Desk
SOR Hit Notice	Answer Hits to SOR

The following is a list of messages which may be spawned from processing a consolidation request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3106 Consolidation Notification
N3112 (MSO) Multi-state Offender Status
N3126 SOR Agency Notice

Figure 21.3-03 External Death Notice Data Flow Sequencing and Notes

This data flow applies to the STOT DEC. This data flow illustrates IAFIS processing of the External Death Notice (NCIC DEC message). Deceased criminal history records remain active in IAFIS until purging occurs at a specified age or after 7 years. Two types of DEC messages can occur. (a) If the death is not substantiated by fingerprints taken from the body, the basic DEC message will be appended with an XPL (explanation) field. This will cause IAFIS to mark the SID as deceased. (b) If the state policy is that it will decease its record only when the death is substantiated by fingerprints taken from the body, the basic DEC message will be appended with an FII (Fingerprint Identification Indicator) field. This will cause IAFIS to decease the entire subject record.

(1) IAFIS receives the III Decease Notification Request-DEC (N3203) message from a state agency via NCIC when it wishes to notify the FBI that a subject is deceased

(2) III/FBI returns either a single-line or multiple-line reject of the request, or an acknowledgment that the subject record was updated as requested in the III Deceased Notification Accept Response-DEC (N3204) message via NCIC.

(3) The following is a list of unsolicited reports that may be spawned from processing an External Death Notice and sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
III Participant Online Printer Response—Hit Against SPF 5, 6, C, K, N, or DOD	Special Stops Unit (5 or 6 or C or N) Document Specialist (K or DOD w/ XPL)
III Participant Online Printer Response—Hit Against Missing Person, Amnesia	Answer Hits to Wants (I or T)

Report Title	Destination Printer
Victim or Wanted Subject	
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
Record Set Report	Dead Desk (DOD w/ FII)

Note: When a subject record is deceased, III/FBI provides unsolicited notification to agencies associated with the subject.

Note: III/FBI will send an unsolicited Hit to Want Notification (N3401) message when the deceased subject record contains a Want.

Note: If the subject record is deceased and it contains Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) to all registering agencies.

The following is a list of unsolicited messages that may be spawned from processing a DEC request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/ Name
N3107 Unsolicited Deceased Notification
N3121 (SSO) Single State Offender Status Notification
N3124 Unsolicited Activity Notification
N3401 Hit to Want Notification
N3126 SOR Agency Notice

Figure 21.3-04 Internal Death Notice Data Flow Sequencing and Notes

This thread is not used, has not been used, had no SP/CRs written against it, and, it has been transitioned to another STOT (SCHD) and message number (A3038).

This DFD applies to the STOT DEAD. This data flow illustrates IAFIS processing of an Internal Death Notice document. The flow describes the processing for documents notifying the FBI that an individual is deceased. The document is **not** accompanied by a fingerprint card. Processing for deceased notifications with fingerprint cards is described in the fingerprint card submission flows. IAFIS does **not** change a subject record status to "deceased" based on a document without an associated fingerprint card. An FNU **should** be supplied.

(1) This flow represents the interaction of the DPS Service Provider as the Death Notice activity occurs. The Service Provider requests copies of the criminal history record of the deceased subject and views the results. The Service Provider initiates the Death Notice file maintenance and is given an indication of the success or failure of the request.

(2) ITN/FBI sends a Service Provider Subject Search Request (A1032) message, including the subject FNU, to III/FBI. It is assumed that for Death Notice processing the Service Provider will include only the FNU and no other subject data, initiating a direct retrieval of the record for the desired subject. If the FNU is not provided, an A1032 may be initiated containing other identifiers or descriptors in order to obtain an FNU. If an FNU cannot be determined for this subject, the Death Notice document will be returned to the submitter.

(3) If zero or more than one candidate is to be returned to ITN/FBI or if A1032 contained a value of 'Y' in CAND-LIST-FLAG, III/FBI will return a Service Provider Subject Search Candidate List (A1029) message that contains descriptive data for each candidate (if not zero). The Service Provider may then submit another A1032 message containing the FBI number of the candidate selected from the list. If a single candidate is to be returned to ITN/FBI and if A1032 contained a value of 'N' in CAND-LIST-FLAG, III/FBI will return a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

NOTE: Refer to DFD 21.4-04 Sequencing and Notes for further detail regarding the conditions and use of messages A1032, A1029, and A1033.

(4) The Death Notice File Maintenance Request (A3030) message contains the FBI number of the deceased subject, the subject date of birth (for verification of the subject identity), date of death as provided on the initiating document, and the ORI. If filtering reveals a Special Stop subject, and the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A3030 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3030.

(5) III/FBI modifies the subject record if able to do so, and returns a File Maintenance Response (A3027) message to ITN/FBI.

(6, 7) If a hard copy response is desired and the subject record contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states. The state data is returned in the Nlets CR Response (L1048).

(8) III/FBI will produce a hard copy if it has been requested. If a Service Desk provider or Special Stops provider is processing the action, III/FBI may generate an Unsolicited Report (A3150) message in addition to or instead of printing a hardcopy report on the III/FBI high-speed printer.

Report	Destination Printer
IDRR/NIDR	Special Stops Unit

Report	Destination Printer
IDRR/NIDR	Service Desk

Figure 21.3-06 Internal Disposition Report Data Flow Sequencing and Notes

This DFD applies to the STOTs DSPD and DSPM. This diagram illustrates IAFIS processing of document and MRD dispositions.

Document Dispositions start from this point:

This flow represents the interaction of the DPS Service Provider as the Disposition Report activity occurs. The Service Provider requests copies of the criminal history record of the subject and views the results. The Service Provider initiates the disposition file maintenance and is given an indication of the success or failure of the request.

(1) ITN/FBI sends a Service Provider Subject Search Request (A1032) message to III/FBI which contains an FBI number.

(2) III/FBI will return a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

(3) The Disposition File Maintenance Request (A3036) message sent to III/FBI contains the FBI number of the subject and disposition information as provided on the document. If filtering reveals a Special Stop subject, and the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A3036 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3036.

Electronic (MRD) Dispositions continue from this point:

(4) III/FBI modifies the subject record if able to do so, and returns a File Maintenance Response (A3027) message to ITN/FBI.

(5) Document Only: If the A3036 attempts to update a record containing a Want and if the subject is a Bureau fugitive (including SPF = 'I' or 'T'), III/FBI completes the requested file maintenance. III/FBI then generates a Review Request (A1312) message that will be routed to a DPS Service Provider for review and processing.

(6) The Service Provider releases the transaction for response generation after the review and any necessary modifications by sending the Review Response (A1313) message to III/FBI.

(7)Document Only: If the subject record is to be provided and contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(8) The state data is returned in the Nlets CR Response (L1048).

(9) III/FBI may print one or more copies of the subject criminal history record for mailing to interested agencies. If a Service Desk provider or Special Stops provider is processing the action, III/FBI may generate an Unsolicited Report (A3150) message in addition to or instead of printing a hardcopy report on the ITN/FBI printer.

Report	Destination Printer
IDRR/NIDR	Special Stops Unit
IDRR/NIDR	Service Desk

NOTE: III/FBI performs filtering; if filtering reveals a Special Stop subject with an SPF of '5,' III/FBI prepares an Unsolicited Report (A3150) message for the Special Stops Unit and an Unsolicited Activity Report (N3124).

(10) MRD Only: III/FBI writes MRD responses (acknowledgments) to tape and prints a hard copy summary report to be returned to the submitter with the tape.

The following is a list of messages which may be spawned from processing an MRD Disposition Request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/ Name
N3124 Unsolicited Activity Notification

The following is a list of unsolicited reports that may be spawned from processing an MRD Disposition. These reports will be formatted by III/FBI and printed on desktop printers in ITN/FBI.

Report	Destination Printer
III Participant Online Printer	Special Stops Unit
Response—Hit Against SPF 5, 6, C, K, N, or DOD	Document Specialist
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
MRD Disposition Request Online Printer Response—Hit Against SPF 5 or 6 or C or N	Special Stops Unit

Figure 21.3-07 External Expungement Request Data Flow Sequencing and Notes

This DFD applies to the STOT DRS. This diagram illustrates IAFIS processing of an External Expungement (NCIC DRS message).

If the request comes from an NFF state, III/FBI will wait for one hour to allow the state to reverse the expungement. Then, III/FBI will complete the expungement as if it were a document. When the request comes from a non-NFF state, III/FBI will automatically reverse the arrest cycle expungement if an associated expungement document has not been processed within 30 days of receipt of the DRS message. This diagram includes the unsolicited messages that would be sent if the expungement is automatically reversed. Refer to the Internal Expungement Request Data Flow diagram (Figure 21.3-08) for processing of the follow-up expungement document.

(1) IAFIS receives a III Expungement Notification Request (N3205) message via NCIC from a state agency when it wishes to expunge arrest cycles for a subject.

NOTE: III/FBI performs filtering; if filtering reveals a Special Stop subject, III/FBI prepares an Unsolicited Report (A3150) message for the Special Stops Unit. An Unsolicited Activity Report (N3124) is generated when the SPF is '5.'

If the expungement modifies the record of a subject containing a Want (SPF='I' and 'T' only), III/FBI completes the requested file maintenance. If the record contains these Wants AND the DRS is from an NFF state, III/FBI will send a III Participant Online Printer Response—Hit Against Missing Person, Amnesia Victim or Wanted Subject Report via an Unsolicited Report (A3150) message to the Hits to Wants printer (see Unsolicited Reports below). If the expungement removes the last arrest cycle from an SCH record containing a want (SGT = 'W'), III/FBI will set the AUD = 'P.' If the expungement removes the last arrest cycle from an SCH record containing Sexual Offender Registry Data, III/FBI sends a Record Expunged Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) to all registering agencies.

The following is a list of unsolicited reports that may be spawned from processing an external expungement. These reports will be formatted by III/FBI and printed on desktop printers in ITN/FBI. These reports may also be generated if an expungement must be reversed after 30 days.

Report Title	Destination Printer
III Participant Online Printer Response—Hit Against SPF 5, 6, C, K, N, or DOD	Stops Unit (5) Document Specialist (K)
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
III Participant Online Printer Response—Hit Against Missing Person, Amnesia Victim or Wanted Subject Report	Answer Hits to Wants

(2) III/FBI sends an Expungement Notification Accept Response—DRS (N3206) message, via NCIC to the requester. This response will contain either a single-line or multiple-line reject of the request or an acknowledgment that the subject arrest cycles have been expunged as requested.

(3) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI in three unique situations with respect to external expungements:

a) If the expungement request was from an NFF state and the last arrest cycle was expunged, III/FBI initiates file synchronization with ITN/FBI so that the fingerprint images and features data will be marked as deleted.

b) If the expungement request does not expunge an entire subject record, because the subject has other active arrests, the expungement of arrest cycles for that state may change the subject descriptive data by deleting some AONs. If so, the A3045 will contain descriptive data to pass to AFIS/FBI.

c) If the expungement must be reversed after 30 days, III/FBI will reactivate the expunged arrest cycles. Again, this may change the subject descriptive data by adding some AONs. If so, the A3045 will contain descriptive information to pass to AFIS/FBI.

(4) ITN/FBI sends a Delete Fingerprint Features Request (A3321) message to AFIS/FBI to delete the fingerprint features and descriptive data when expunging a subject, or an Update Descriptive Data Request (A3312) message to update the descriptive data of the subject.

The following is a list of messages which may be spawned from processing an External Expungement Request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name	
N3108	FNU Expungement Notification
N3109	SID Expungement Notification
N3121	Single State Offender Status Notification
N3124	Unsolicited Activity Notification
N3126	SOR Agency Notice

If the expungement document is not received from the non-NFF state within 30 days, the following unsolicited messages may be spawned.

Message Number/Name	
N3112	(MSO) Multistate Offender Status
N3118	Reactivate Expunged Cycles Notification

Figure 21.3-08 Internal Expungement Request Data Flow Sequencing and Notes

This DFD applies to the STOTs EXPD and EXPM. This data flow illustrates IAFIS processing of an Internal Expungement document. These documents are produced by arrest or judicial agencies when a person has been exonerated after initial arrest or released without charge and disposition as such. An expungement is a request by the court, arresting agency, or state bureau to remove the incident from the criminal history files held by the FBI.

This flow represents the interaction of III/FBI with MRD or the interaction of the DPS Service Provider as the expungement activity occurs. The Service Provider requests a copy of the criminal history record of the subject and views the results. The Service Provider initiates the Expungement file maintenance and is given an indication of the success or failure of the request.

(1) ITN/FBI sends a Service Provider Subject Search Request (A1032) message, including the subject FNU to III/FBI. It is assumed that for Expungement processing, the Service Provider will include only the FNU and no other subject data, initiating a direct retrieval of the record for the desired subject.

(2) III/FBI will return a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject. **(Does not apply to MRD)**

(3) ITN/FBI sends the Expungement File Maintenance Request (A3029) message containing the FBI number of the subject and the identifier for the arrest that is being expunged to III/FBI. One arrest is expunged by this message. If filtering reveals a Special Stop or SPF = 'K' subject, and the transaction has not been initiated by the Special Stops Unit (for SPF = '5' or '6' or 'C' or 'N') or Doc Spec (for SPF = 'K'), III/FBI will reject A3029 with an A1802 for Unauthorized Access. When this rejection occurs, the Service Provider will carry the transaction document(s) to the Special Stops Unit or Doc Spec, as appropriate, for review. Upon completion of the review, the Service Provider will resubmit A3029. **(Does not apply to MRD)**

(4) Document only: If the expungement attempts to remove the last cycle for a subject, and that record contains any Want, III/FBI terminates the requested file maintenance and sends an Error Notification (A1802) message to ITN/FBI where the initiating document(s) will be routed to the appropriate Service Provider for review and processing. If the expungement attempts to remove the last cycle for a subject, identified as a sexual offender, III/FBI terminates the requested file maintenance and sends an Error Notification (A1802) message to ITN/FBI where the initiating document(s) will be routed to Doc Spec for review and processing.

(5) Document Service Provider: III/FBI modifies the subject record if able to do so and returns a File Maintenance Response (A3027) message to ITN/FBI.

(6) Document only: If filtering revealed a Special Stop subject or a record containing SPF = 'K' or a Want (SPF = 'I,' 'L,' or 'T'), AND the action is an MRD expungement, a message will be written to the tape stating that the request will be processed manually and an A3150 will be routed to a Special Stops Service Provider, Document Specialist, or Want Service Provider as appropriate for processing.

(7) Document only: If the expungement requests modification of the record of a subject containing a Want (SPF = 'I,' 'T' only), III/FBI completes the requested file maintenance. III/FBI then sends a Review Request (A1312) message to ITN/FBI.

The following is a list of unsolicited reports that may be spawned from processing a document expungement and sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on desktop printers in III/FBI.

Report Title	Destination Printer
MRD Expungement Hit	Document Specialist (K or

Report Title	Destination Printer
Against 5, 6, C, K, N, DOD, Missing Person, Unknown Deceased, Amnesia Victim, or Wanted Subject	DOD) Special Stops Unit (5 or 6 or C or N) Answer Hits to Wants (Wanted Subject)
IDRR	Service Desk/Liaison Unit Document Specialist Answer Hits to Wants Special Stops

NOTE: If an MRD expungement removes the last arrest cycle from an SCH record containing Sexual Offender Registry (SOR) data, III/FBI sends a Record Expunged Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) to all Registering agencies.

(8) If an A1312 was sent in flow (7), the Service Provider releases the transaction for response generation after the review and any necessary modifications by initiating a Review Response (A1313) message for delivery to III/FBI.

(9) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI under the following circumstances:

a) If the expungement changes the subject descriptive data by deleting an arrest offense, III/FBI sends new descriptive data in A3045 to ITN/FBI to pass to AFIS/FBI;

or

b) If the expungement removes the last active arrest cycle for the subject, III/FBI notifies ITN/FBI via A3045 to delete fingerprint images and to have AFIS/FBI delete the associated features.

(10) ITN/FBI sends either a Delete Fingerprint Features Request (A3321) message to AFIS/FBI, requesting deletion of the fingerprint features and descriptive data when expunging a subject or an Update Descriptive Data Request (A3312) message to update the descriptive data for the subject.

(11) If the subject record is to be provided and contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(12) The state data is returned in the Nlets CR Response (L1048).

(13) Document Service Provider: III/FBI provides a hardcopy criminal history record report to agencies associated with the subject.

If a Service Desk provider, Document Specialist, Wants provider, or Special Stops provider is processing the action, III/FBI may receive a request to send an Unsolicited Report (A3150) message to an ITN/FBI printer in addition to or instead of printing a hardcopy report on the ITN/FBI printer.

Report	Destination Printer
IDRR/NIDR	Special Stops Unit
IDRR/NIDR	Document Specialist
IDRR/NIDR	Answer Hits to Wants
IDRR/NIDR	Service Desk

MRD: III/FBI writes MRD results to tape and prints a hard copy summary report.

The following is a list of messages which may be spawned from processing an

internal expungement request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

N3108 FNU Expungement Notification
N3109 SID Expungement Notification
N3121 (SSO) Single State Offender Status Notification
N3124 Unsolicited Activity Notification
N3126 SOR Agency Notice

Message Number/Name

Figure 21.3-10 Freedom of Information Act Request Data Flow Sequencing and Notes

This data flow applies to the STOTs FOID and LCAR and the TOT FIDO. A request made under the Freedom of Information Act (FOIA) for subject records held by the FBI may consist of a request for all criminal history information (which will include any active 'local' wants), and/or all civil information and/or reproductions of ten-print finger images. FIDO submissions will follow the message sequence for those messages specific to submissions received through the CSS facility and transmitted to IAFIS via the CJIS WAN (DFD 21.1-01d). At the conclusion of processing (for FOIDs only), if the responses were indicated to be returned locally, the initiating Service Provider will collect the reports, images, and the original submission, merge them and prepare the response for return to the submitter. Otherwise, III/FBI will prepare responses according to the CCA File entry for the submitting agency and print to the high-speed printer.

The initiating Service Provider (DPS or LPS) scans the fingerprint card accompanying the FOIA request or criminal submission on a local ITN/FBI scanner and enters biographic and descriptive data; the Service Provider may include an FNU. FBI Latent Specialists (FAS only—this function is not available to OFOs) may initiate a criminal submission (STOT LCAR) using either an electronically submitted ten-print received as STOT MCS or CFS (which may require the entry of additional data, DOA, etc., if not included with the latent submission), or a ten-print card. For FOID STOT the ORI is set to the FOIA ORI and for FIDO the ORI is set to WVFBICS4Z.

(1) (For FIDO only) The EBTS Ten-Print Submission (E1000) message is received by IAFIS from the CSS via the CJIS WAN. The TOTs carried by E1000 as depicted in this diagram will be unique to the CSS (refer to the E1000 message definition and the TOT Code Table, contained in the IAFIS MDD.)

(2-10) Normal Ten-Print submission processing proceeds (see DFDs 21.1-01a).

(11) ITN/FBI sends a Ten-print Criminal History File Maintenance Request (A3026) to III/FBI to perform file maintenance and/or response generation as required. The 'PCC' value in A3026 may be set to 'B' by the Service Provider (STOT FOID only), which will cause the response to be returned directly to that Service Provider. ITN/FBI will place the appropriate printer location code in the field 'RPTDEST;' III/FBI will use this value to route the response to the proper printer.

STOT FOID and TOT FIDO only: If the transaction is an Ident to the criminal file, it is treated as a normal Civil Retain, i.e., a cycle is added to the III/FBI Subject Criminal History file, ITN/FBI updates the TPCF, and AFIS/FBI features and descriptive data are updated.

(12) (TOT FIDO only) III/FBI will direct these hard copy responses to the high-speed printer under a 'FOIA/FIDO RESPONSES TO FOLLOW' Banner Page and simultaneously send ITN/FBI an A1003. ITN/FBI converts the message to an E1003 and sends it to EFCON/FBI. EFCON/FBI then sends the E1003 Card Disposition Response CSS (CRDC) containing the Card Disposition (CDDISP) of 'R' (Return with Response) to the CSS via the CJIS WAN. This informs the CSS that the transaction is complete and the action to be taken with the card.

STOT LCAR only: If the transaction is an Ident to the criminal file, it is treated as a normal Criminal Ident Retain, i.e., a cycle is added to the III/FBI Subject Criminal History file, ITN/FBI updates the Ten-Print Certification File, and AFIS/FBI features and descriptive data are updated.

If filtering reveals a Special Stop subject, and the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A3026 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. **If the Special Stops review results in a decision to Non-Ident the candidate with the submission, no A3314 will be sent.** Upon completion of the review, ITN/FBI will resend A3026.

(13) If a subject record (in a criminal Idented submission) contains NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(14) The state data is returned in the Nlets CR Response (L1048) message. These flows occur only when a copy of the subject record is to be provided.

(15) If the A3026 attempts to update an SCH record containing a Want, III/FBI suspends the criminal record response generation until its release by the Service Provider. III/FBI will send a Review Request (A1312) message to ITN/FBI that will be routed to a DPS Service Provider for review and processing.

*****III/FBI generates and sends a QTP Request Message to NCIC following the start of File Maintenance and after the completion of any required manual reviews.**

(16) The result of the DPS Service Provider review is a Review Response (A1313) message sent from ITN/FBI to III/FBI.

NOTE: For FIDO and FOID only - The A1313 may direct III/FBI to send a Non-Deceased Fingerprint Card On-Line Hit Notification report via an unsolicited Hit to Want Notification (N3401) to the Want Originator.

(17) III/FBI will return the Ten-print File Maintenance Response (A3025) message to ITN/FBI in response to the A3026. The A3025 Ten-Print File Maintenance Response message notifies ITN/FBI to update the Criminal Fingerprint Image Master File, as appropriate, and to start the update with AFIS/FBI.

LCAR only: Upon receipt of the A3025, ITN/FBI will send an e-mail message containing the ICN and FNU (if applicable) to the Latent Specialist. No other response is produced locally for this submission.

(18) To provide automated criminal records when the initiating Service Provider has indicated that the response be returned locally, III/FBI will send an Unsolicited Report (A3150) to ITN/FBI. A criminal IDRR will include criminal data, arrest data ("rap sheet") and Want information, as appropriate. Alternately, III/FBI will send an NIDR if no releasable criminal information exists. Photos stored in the IPS in III/FBI are not included.

The following is a list of unsolicited reports that may be sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Unsolicited Report	Destination Printer
IDRR/NIDR	Special Correspondence

(19) If the transaction results in an Ident to the criminal file, the Update Fingerprint Features Request (A3310) message will be sent to AFIS/FBI. **Otherwise, the A3310, A3311, and A3331 messages are not sent.** A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI. The image file is formatted per I3020. AFIS/FBI updates features, if better, and descriptive information in the Criminal Master File.

NOTE: If the submission was Idented to a criminal record and AFIS/FBI upgrades its features, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Unsolved Latent Search Data Flow (Figure 21.1-08).

(20) AFIS/FBI will return the Update Fingerprint Features Response (A3311) message to ITN/FBI.

(21) ITN/FBI sends the File Maintenance Completion Notification (A3331), which includes the pattern classification and ten-print certification pointer. III/FBI does not respond to this message.

NOT SHOWN: If requested, the Service Provider may print copies of ten-print images. The service provider will compile the criminal records and fingerprint images, as requested, to provide to the requester. The A1040, A1042, and A3150 messages may also be used by the Service Provider to obtain criminal records (refer to DFD 21.4-04).

NOTE: If the submitter did not request criminal information, the service provider will omit any IDRR produced from the written response.

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3401 Hit to Want Notification
N3107 Unsolicited Deceased Notification
N3112 Multi-state Offender Status
N3114 Non-matching SID Ignored
N3115 No Prior Record – SID Entered
N3116 Prior Record – Previously Entered SID Notification (Single)
N3117 Prior Record – SID Entered
N3119 Reject, No Prior Record, SID Not Entered
N3120 Reject, Prior Record, SID Not Entered
N3123 Prior Record – Previously Entered SID (Multi)
N3126 SOR Agency Notice

Figure 21.3-12 Internal Record Sealing Request Data Flow Sequencing and Notes

This DFD applies to the STOT RSD. This data flow illustrates IAFIS processing of an Internal Record Sealing Request. This flow describes the processing for documents notifying the FBI that one or more arrest cycles for a subject must be sealed. This process can also be used to notify the FBI to unseal an arrest cycle(s) to allow dissemination.

This flow represents the interaction of the DPS Service Provider as the Record Sealing activity occurs. The Service Provider requests copies of the criminal history record for the subject and views the results. The Service Provider initiates the Record Sealing file maintenance and is given an indication of the success or failure of the request.

(1) ITN/FBI sends a Service Provider Subject Search Request (A1032) message to III/FBI which will contain an FBI number. III/FBI will retrieve the subject record if the FBI number is provided, and will also perform a name search if descriptive data is present in the request.

(2) III/FBI returns a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject. For a valid FBI number that is not found in the file, the A1033 will contain the associated AUD code.

(3) The Service Provider initiates a Record Seal File Maintenance Request (A3040) message sent to III/FBI containing the FBI number of the subject and up to 10 arrest cycle identifiers indicating the cycles to be sealed or unsealed. If filtering reveals a Special Stop subject, and the transaction has not been reviewed by the Special Stops Unit, III/FBI will reject the A3040 with an A1802 for Unauthorized Access. When this rejection occurs, the Service Provider will manually route the request to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3040.

(4) If the A3040 attempts to update a record containing an I/O or Bureau Fugitive Want, III/FBI completes the requested file maintenance. III/FBI then generates a Review Request (A1312) message that will be routed to a Wants Service Provider for review and processing.

(5) The Service Provider releases the transaction for response generation after the review and any necessary modifications by sending the Review Response (A1313) message to III/FBI.

(6) III/FBI modifies the subject record if able to do so and returns a File Maintenance Response (A3027) message to ITN/FBI.

(7) If the subject record is to be provided to the requesting agency and contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(8) The state data is returned in the Nlets CR Response (L1048).

(9) If a DPS or Special Stops provider is processing the action, III/FBI may generate an Unsolicited Report (A3150) message for the following in addition to or instead of printing a hardcopy report on the III/FBI printer:

Report	Destination Printer
IDRR/NIDR	Service Desk
IDRR/NIDR	Special Stops Unit

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a des-

tination outside IAFIS via the NCIC telecom network.

N3121 - Single State Offender Status Notification

Message Number/Name

Figure 21.3-13 Internal SCH Modification Request Data Flow Sequencing and Notes

This DFD applies to the STOTs SCHD and SSMD. This diagram illustrates IAFIS processing of the SCH Modification. These requests are typically used to correct mistakes found in an SCH file record. Within defined constraints they may be used to add, modify, or delete any field in an SCH record. In particular, arrest charges or complete arrest cycles can be deleted, effectively accomplishing a full or partial expungement.

This flow represents the interaction of ITN/FBI with the DPS Service Provider as the SCH Modification activity occurs.

(1) ITN/FBI sends a Service Provider Subject Search Request (A1032) message to III/FBI which will contain an FBI number. III/FBI will retrieve the subject record if an active FBI number is provided in the request.

(2) If a single candidate is to be provided, III/FBI returns a Service Provider Subject Search Candidate Record (A1033) message which contains the criminal history data for that subject.

(3) If the FBI number provided is not correct, III/FBI will return a Subject Search Response (A1029) with no candidates. At this point the Service Provider can either re-issue the A1032 message with the correct FBI number or reject the process.

(4) The Service Provider will initiate the modification by causing ITN/FBI to send an SCH Modification File Maintenance Request (A3038) message to III/FBI, indicating how the file should be modified. Changes are specified by giving the FNU, field name, an optional old value, and the new value, the type of request, and the record level, as well as data that defines the type of cycle to be changed (refer MDD A3038 Message Definition). If filtering reveals a Special Stop subject, and the transaction has not been reviewed by the Special Stops Unit, III/FBI will reject A3038 with an A1802 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3038.

(5) If a subject record contains NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(6) The state data is returned in the Nlets CR Response (L1048). These flows occur only when a copy of the subject record is to be provided.

(7) If the modification updates the record of a subject containing a Bureau Fugitive want, III/FBI completes the requested file maintenance. III/FBI then sends a Review Request (A1312) message to ITN/FBI that will be routed to a Wants Service Provider for review and processing.

(8) The result of the DPS Service Provider review is a Review Response (A1313) message sent from ITN/FBI to III/FBI.

(9) III/FBI modifies the subject record if able to do so and returns a File Maintenance Response (A3027) message to ITN/FBI.

(10) The Service Provider may request that III/FBI generate an Unsolicited Report (A3150) message if a hardcopy report is needed for mailing to agencies associated with the subject.

Report	Destination Printer
IDRR/NIDR	Special Stops Unit
IDRR/NIDR	Service Desk

(11) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI under the following circumstances:

a) If the modification changes the subject descriptive data, III/FBI sends new descriptive data in the A3045 to pass to AFIS/FBI.

b) If the modification deletes the last active arrest cycle for the subject, III/FBI notifies ITN/FBI via the A3045 to initiate the deletion of fingerprint images and to have AFIS/FBI delete the associated features.

ITN/FBI sends a message to AFIS/FBI to continue file synchronization in the following manner:

(12) To update descriptive data only: ITN/FBI sends an Update Descriptive Data Request (A3312) message to AFIS/FBI.

(13) To delete (expunge) a subject: ITN/FBI sends a Delete Fingerprint Features Request (A3321) message to AFIS/FBI.

The following is a list of messages which may be spawned from processing a SCH Modification that results in an expungement. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3108 FNU Expungement Notification
N3109 SID Expungement Notification
N3121 (SSO) Single State Offender Status Notification

Figure 21.3-14 Restore FNU Request Data Flow Sequencing and Notes

This DFD applies to the STOT RFND. This diagram illustrates how an expunged (AUD = 'E'), deceased (AUD = 'N'), deleted (AUD = 'W'), or consolidated (AUD = 'C,' killed FNUs; AUD = 'BLANK,' kept FNU) subject is restored, if within 30 days. Restoration taking place more than 30 days after the expungement, deletion, consolidation, or deceased action must be re-entered from user-supplied information—***this diagram does not address this process***. Record restorations occur only for subjects in the criminal file and are initiated only internally. Only the most recent restorable action to an FNU may be restored. **No restoration from an NFF state SID expungement may be made. Subjects which were expunged due to a document expungement may be restored; however, this process restores only the last arrest cycle that was expunged in the subject record.**

The DPS Service Provider initiates a query to determine if a file is restorable through an ITN/FBI workstation.

(1) ITN/FBI sends the Restore FNU Query (A1008) message to III/FBI to determine if the given FNU is restorable. If filtering reveals a Special Stop subject and the transaction has not been reviewed by the Special Stops Unit, III/FBI rejects the A1008 with an Error Notification (A1802) message for unauthorized access. If this rejection occurs, ITN/FBI notifies the Special Stops Unit of the request and directs the submitter to route any documents and a screen printout to the Stops Unit supervisor. After reviewing the transaction, the Special Stops Unit may reinitiate the restoration by submitting another Restore FNU Query (A1008).

NOTE: If the record is not restorable from any action (expungement, etc.), III/FBI will return an A1802 containing error code L0002

(2) If the FNU is restorable, III/FBI returns the Restore FNU Query Response (A1009) message to ITN/FBI to report FNU restorability and the process from which it can be restored. If the FNU provided in the A1008 is that of a consolidated subject (i.e., a "kept" FNU), the A1009 will indicate the "killed" FNUs which were consolidated into the "kept" FNU.

If the Service Provider mistakenly entered a "killed" FNU in A1008, the A1009 message includes the "kept" FNU.

(3) If the FNU provided in the A1008 is that of a consolidated subject and ONLY if that record is restorable AND contains post-consolidation changes, III/FBI sends an Unsolicited Report (A3150) message containing the existing record set (the record set as it stands following the consolidation) and post-consolidation changes (if any exist) to the Service Provider for action. Otherwise, III/FBI does not send an A3150.

Report Title	Destination Printer
Post-Consolidation Report	Document Specialist or Special Stops

The Service Provider will request the TPCF entries for all submissions that have been posted to a kept FNU following a consolidation or printout of the record(s) a Criminal History Request (see DFD 21.4-02)..

If the FNU is no longer restorable from the expungement, consolidation, deletion, or deceased activity of interest; or if for some other reasons the Service Provider does not wish to continue, the transaction may be terminated at this point. Otherwise, the following may occur:

(4) ITN/FBI sends the Restore Criminal History Request (A3407) message containing the FNU to be restored and the action from which it is to be restored (expungement, deletion, consolidation, or deceased). If filtering reveals a Special Stop subject and the transaction has not been reviewed by the Special Stops Unit, III/FBI rejects the A3407 with an A1802 message for unauthorized access. When this rejection occurs, ITN/FBI notifies the Special Stops Unit of the request and directs the submitter to route any documents and a screen printout to their supervisor. After reviewing the transaction, the Spe-

cial Stops Unit may reinitiate the restoration by submitting another Restore FNU Query (A1008).

(5) If the FNU is restorable, III/FBI restores the record to its former state (including only those photos active in the IPS at the time of the consolidation or expungement), sets the restorability flag for the subject(s) to non-restorable, and sends ITN/FBI the File Maintenance Response (A3027) message. If the RST in the A3407 does not match the FNU RST in III/FBI, III/FBI rejects the A3407 with an A1802 indicating an RST mismatch. If a restored record contains a Want (SPF = 'I,' 'L,' or 'T'), the File Maintenance Response will also direct the Service Provider to take the transaction documents to Answer Hits to Wants. If restoring a deceased record, the A3027 will direct the Service Provider to take the transaction to the Dead Desk.

NOTE: If SOR information was posted to a record AFTER a consolidation, restoration of the killed FNU(s) will cause the SOR to be lost. When the Restore process is complete, the Service Provider will need to carry the initiating document(s) to the SOR group for the SOR agency to be notified to reestablish the SOR.

NOTE: If restoring a deceased record (AUD = 'N'), no file synchronization is necessary; the processing described in flows (7) through (10) does not occur.

(6) If restoring a deleted, expunged, or consolidated record(s), III/FBI sends the Restore FNU File Synchronization Request (A3046) message to ITN/FBI, providing the FNU(s) to be restored or updated and the accompanying data descriptors. ITN/FBI reactivates the original FIMF record involved in the expungement or deletion. In a restore from consolidation, ITN/FBI reactivates the killed FNU(s) FIMF record(s) and restores the kept FNU FIMF record to its state at the time of consolidation, replacing the consolidated FIMF record of the kept FNU.

(7) ITN/FBI sends an Update Fingerprint Features Request (A3310) message to AFIS/FBI to update features and data descriptors for each restored FNU. The A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the image file from ITN/FBI. ITN/FBI formats the file per I3020. For each expunged, deleted, or killed (in consolidation) FNU being restored, ITN/FBI indicates that AFIS/FBI is to add a new record for the FNU. For the KEPT FNU in a restore from consolidation, ITN/FBI indicates that AFIS is to override the feature quality score and replace the existing features with the features from the supplied images.

(8) For each A3310 received, AFIS/FBI returns to ITN/FBI the Update Fingerprint Features Response (A3311) message which contains an indication of success or failure, and the pattern classification.

(9) For each A3311 received, ITN/FBI sends the File Maintenance Completion Notification (A3331) message to III/FBI, which contains the pattern classification.

NOTE: If a display or printout of the restored record(s) is desired, a Criminal History Request (see DFD 21.4-02) may be used.

The following is a list of messages that may be spawned from processing a Restore FNU Request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3112 Multi-state Offender Status
N3121 Single State Offender Status Notification

NOTE: After an unconsolidation, a Service Provider may verify that the fingerprint records represent more than one subject. The document Service Provider manually re-enters any post-consolidation record changes to the correct subject record(s). If the unconsolidation request was in error, or if the Service Provider performed the unconsolidation to consolidate into a different "kept" FNU, the Service Provider consolidates the records with the consolidation process (DFD 21.3-02) and manually re-enters any changes to the record reported in the Post-Consolidation Report (manual re-entry is not part of the workflow).

Figure 21.3-16 External Criminal Print Ident Data Flow Sequencing and Notes

This DFD applies to the STOT CPI. This diagram illustrates an NFF participant Criminal Print Ident (CPI) request and response. In this flow, the NFF participant is notifying the FBI that a criminal Ident was made at the state level for a given FNU and SID. The FBI will respond to the NFF participant with a III CPI Accept Message.

(1) III/FBI receives the III Criminal Print Ident Request-CPI (N3213) message via NCIC when an NFF participant wishes to notify the FBI that an Ident was made at the state level for a given FNU and SID.

If the N3213 references a record containing a Want, III/FBI sends a III Ident Message—Online Hit Notification report via an unsolicited Hit to Want Notification (N3401) message to the Want originator and the CPI originator. III/FBI then proceeds with response generation.

If the N3213 references a record containing Sexual Offender Registry (SOR) data, III/FBI sends a Fingerprint Identification Sexual Offender Registry Agency Notice(s) via an SOR Agency Notice (N3126) message to all registering agencies.

(2)III/FBI will perform filtering. If filtering reveals a Special Stop subject containing an SPF of '5' or '6,' III/FBI prepares an Unsolicited Report (A3150) message for the Special Stops Unit and an Unsolicited Activity Report (N3124) message. If III/FBI detects a Special Stop subject containing an SPF of 'C' or 'N,' III/FBI will send an Unsolicited Report (A3150) message to ITN/FBI to be generated in the Special Stops Unit. If filtering reveals an SPF = 'K' or DOD, III/FBI prepares an Unsolicited Report (A3150) message and routes it to Doc Spec. (See Unsolicited Reports and Unsolicited Messages, below.)

The following is a list of unsolicited reports that may be sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

(3) If the N3213 references a record with a Flash, III/FBI will print an IDRR which will be sent to the Flash originator. **If this record contains NFF cycles, message flows (6) and (7) will occur at this time.**

(4) III/FBI notifies the NFF participant that the request was received by sending a Criminal Print Ident Accept Response-CPI (N3214) message to the requestor via NCIC.

(5) The following is a list of unsolicited reports that may be spawned from processing an External III Criminal Print Ident Request-CPI. These reports will be formatted by III/FBI, sent in the Unsolicited Reports (A3150) message, and printed on desktop printers in ITN/FBI.

Report Title	Destination Printer
III Participant Online Printer Response—Hit Against SPF 5, 6, C, or N	Special Stops Unit (5 or 6 or C or N)
SPF 'K' or DOD	Document Specialist (K)
IDRR/NIDR	Answer Hits to Wants

(6) If the subject record is to be provided and contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(7)The state data is returned in the Nlets CR Response (L1048).

Responses are transmitted to all states having an interest in this subject in accordance with the information contained in the III/FBI CCA file; some states

may be electronic subscribers, some hardcopy.

The following is a list of unsolicited messages which may be spawned from processing an External III Criminal Print Ident (CPI) Request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification
N3401 Hit to Want Notification
N3126 SOR Agency Notice

Figure 21.3-21 Partial Expungement Request Data Flow Sequencing and Notes

This DFD applies to the STOT PEXD. This data flow illustrates IAFIS processing of a partial expungement document. This process is used when one or more charges are dropped from a date of arrest, **however arrest charges will remain for that date of arrest.** If the expungement will remove the last arrest(s) from the date of arrest or record, this process will be rejected.

This flow represents the interaction of the DPS Service Provider as the expungement activity occurs.

(1) ITN/FBI sends a Service Provider Subject Search Request (A1032) message to III/FBI which must contain the FBI number.

(2) III/FBI will return a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

(3) The Service Provider initiates the Partial Expungement Request (A3009) message containing an FBI number and date of arrest, and possibly other arrest data, to III/FBI. If this represents an attempt to expunge the last arrest charge, then an A1802 error is returned and this process is terminated. If filtering reveals a Special Stop subject, and the transaction has not been reviewed by the Special Stops Unit, A1802 will reject A3009 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3009. Up to 39 charges may be included for expungement.

(4) If the expungement applies an update to a record containing a Bureau Fugitive Want, III/FBI performs the requested record update and sends the Review Request (A1312) message to ITN/FBI. The A1312 will be routed to a DPS Service Provider for review and processing.

(5) The result of the DPS Service Provider review is a Review Response (A1313) message sent from ITN/FBI to III/FBI.

(6) If the file maintenance action was successful, III/FBI sends the File Maintenance Response (A3027) message to ITN/FBI.

(7) III/FBI also sends the File Synchronization Request (A3045) message to ITN/FBI containing updated arrest information to pass to AFIS/FBI.

(8) If the subject record contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(9) The state data is returned in the Nlets CR Response (L1048).

(10) ITN/FBI sends an Update Descriptive Data Request (A3312) message to AFIS/FBI.

(11) The Service Provider may request that III/FBI generate an Unsolicited Report (A3150) message if a hardcopy report is needed for mailing to agencies associated with the subject.

Report Title	Destination Printer
IDRR/NIDR	Service Desk
IDRR/NIDR	Special Stops Unit

The following is a list of messages which may be spawned from processing a Ten-Print Submission. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3108 - FNU Expungement Notification
N3109 - SID Expungement Notification
N3121 - Single State Offender Status
N3124 - Unsolicited Activity Notification
N3126 - SOR Agency Notice

Figure 21.3-22 Special Stops Modification Notice Data Flow Sequencing and Notes

This diagram applies to the STOT SSMD and illustrates the process which authorized Service Providers use to create an AUD 'T' record, to change an Inactive FNU (AUD 'W') record to AUD 'T,' to change an AUD 'P' record to AUD 'T,' or to change an AUD 'T' record to AUD 'P'.

This flow represents the interaction of the authorized service provider with the system as the file maintenance is performed. The service provider may retrieve the existing subject record, submit the file maintenance request, and receive the response. If changing an AUD 'T' record to AUD 'P,' the authorized service provider scans in fingerprint images.

If the authorized service provider needs to change a record to AUD 'W' prior to changing the AUD 'W' to AUD 'T,' the service provider will use an SCH Modification Request (see DFD 21.3-13).

(1) The authorized service provider (ITN/FBI) may first query the existing record by sending a Service Provider Subject Search Request (A1032) message to III/FBI, which must contain an FBI number..

(2) III/FBI will return a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

(3) The authorized service provider (ITN/FBI) sends a Special Stops File Maintenance Request (A3041) specifying the desired type of action to III/FBI. When creating an AUD 'T' record, the authorized service provider may specify the FNU, or may allow ITN/FBI to automatically assign a new FNU. The authorized service provider may also set SPF codes using A3041.

If filtering reveals a subject with SPF = '5' or '6' or 'C' or 'N,' or with AUD = 'T,' and the transaction was not sent by an authorized service provider, A1802 will reject A3041 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to the Special Stops Unit for review. Upon completion of the review, ITN/FBI will resend A3041.

Only authorized service providers may use the A3041. In addition to Special Stops service providers, a Hit to Wants service provider may also use this process by having a separate Special Stops Unit log-on (with a Special Stops AUTH code) in addition to the Answer Hits to Wants Unit log-on.

(4) If III/FBI was able to perform the action, It returns a File Maintenance Response (A3027) in response to A3041.

If the A3041 created an AUD 'T' record, or changed an AUD 'W' record to AUD 'T' (TYS = 'U' for each of these actions), the process is complete at this point.

To complete the process to change an AUD 'P' record to AUD 'T' (TYS = 'D'), the following steps are performed:

(5) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI to direct the removal of fingerprint images and features.

(6) ITN/FBI sends a Delete Fingerprint Features Request (A3321) message to AFIS/FBI.

The process to change an AUD 'P' record to AUD 'T' is complete at this point.

To complete the process to change an AUD 'T' record to AUD 'P' (TYS = 'E'), the following steps are performed:

(7) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI to direct the addition of fingerprint images and features.

(8) ITN/FBI sends an Update Fingerprint Features Request (A3310) message, with AAC = '1,' to AFIS/FBI to add fingerprint features. A3310 contains the FILEHANDLE which AFIS/FBI uses to retrieve the file containing images from ITN/FBI. The image file is formatted per I3020.

NOTE: When changing an AUD T record to AUD P, with the addition of fingerprint images to its database, AFIS/FBI initiates a search of the Unsolved Latent File. If the search of the Unsolved Latent File results in a candidate, IAFIS will continue processing as described in the Ten-Print-Initiated Search of Unsolved Latent File Data Flow (Figure 21.1-08).

(9) AFIS/FBI returns an Update Fingerprint Features Response (A3311), containing the pattern classification to ITN/FBI.

(10) ITN/FBI sends the File Maintenance Completion Notification (A3331), with pattern classification to III/FBI.

Figure 21.3-23 Master Record Conversion Data Flow Sequencing and Notes

This DFD applies to the MRCD STOT. This data flow illustrates IAFIS processing for converting a single-cycle or multiple-cycle criminal record in the Manual File. This application does not capture ten-print certification information. The original hard copy ten-print cards will be retained by the FBI.

NOTE: This application is meant to reduce the number of FNUs that must be converted via the service desk log conversion application. The Service Providers (SP) must manually compare the hard copy card with the Subject Criminal History. Any changes to master name must be done via the SCH Mod application (see DFD 21.3-13).

(1) The SP must first query the existing record by sending a Service Provider Subject Search Request (A1032) message to III/FBI, which must contain an FBI number.

(2) III/FBI will return a Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

(3) The SP initiates the ITN/FBI Record Conversion File Maintenance Request (A3023) after each cycle added.

(4) III/FBI performs file maintenance, sets AUD='BLANK,' responds with File Maintenance Response (A3027), and updates the descriptive data in the Subject Criminal History.

(5) III/FBI sends a File Synchronization Request (A3045) message to ITN/FBI to direct the addition of fingerprint images and features.

(6) ITN/FBI sends an Update Descriptive Data Request (A3312) message.

The following is a list of messages which may be spawned from processing Master Record Conversion Documents. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3112 Multistage Offender Status
N3114 Non-matching SID Ignored
N3115 No Prior Record—SID Entered
N3117 Prior Record—SID Entered
N3119 Reject, No Prior Record, SID Not Entered
N3120 Reject, Prior Record, SID Not Entered
N3121 Single State Offender Status Notification

Figure 21.4-01 External Criminal History Request Data Flow Sequencing and Notes

This DFD applies to the STOT QR. This data flow depicts the actions that take place when a NCIC user requests a criminal history for a subject in the Subject Criminal History File.

(1) IAFIS receives the III Criminal History Request-QR (N1045) message via the NCIC system. The request will contain an FBI or SID number.

(2) III/FBI will perform filtering. If filtering detects a Special Stop subject with an SPF of '5,' '6,' 'C,' or 'N' III/FBI sends an Unsolicited Activity Report (N3124) message via the NCIC network. III/FBI will retrieve the subject criminal history record along with any state pointers and will send the Criminal History Request Response—QR (N1046) message to the requester via the NCIC network. This message notifies the requestor that an IDRR will be forthcoming and will list any states that will be providing criminal histories directly to the requestor. III/FBI will forward the III QR Response (N1046) message to the requestor via the NCIC network.

(3) An Unsolicited Criminal History Request (N3105) message is sent via NCIC to any states that have a criminal history on the subject. These states will respond directly to the requestor.

(4) The XML format for the Basic IDRR is based on the Interstate Criminal History Transmission Specification with the exception of Legat and NICS ORIs. The criminal history record (IDRR) is prepared by III/FBI and returned through Nlets (L1306) for merging with any state criminal history before being delivered to the requesting agency.

(5) The criminal history report (IDRR) is prepared by III/FBI and sent as the Criminal History Record Response (N1306) message. III/FBI sends the report via NCIC to the requestor containing any criminal history maintained by the FBI.

(6) The following is a list of unsolicited reports that may be spawned from processing an External Criminal History and sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
III Participant—Multiple FNUs for One III-STATE-POINTER	III Staff Printer
III Participant QH/QR/ZI/ZR/ZRS/QWI Response – FBI Research and Advise	III Staff Printer

The following is a list of messages which may be spawned from the processing of a Criminal History Request.

The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 21.4-02 Internal Criminal History Request Sequencing and Notes

This diagram applies to the STOT RRD, and illustrates the messaging sequence used when a Service Provider requests a subject IDRR, NIDR, Record Set, or RANR from III/FBI. As part to NICS efficiency phase II, this functionality has been extended to NICS service providers working at NICS workstations

This flow represents the interaction between the Service Provider and IAFIS. The Service Provider makes the request and may receive a displayed response on the workstation.

(1) ITN/FBI or NICS sends the Criminal History Request (A1040) message to III/FBI, specifying the type of request: IDRR, NIDR, Record Set, or RANR. If the requester is an Other Federal Organization (OFO) user (determined by AUTH code), III/FBI will only include subjects whose records contain an AUD = 'BLANK' or 'M;' further, OFO user requests for NIDR, Record Set, or RANR will be rejected as invalid.

NOTE: III/FBI performs filters for Special Stop subjects (SPF = '5' or '6' or 'C' or 'N'). When III/FBI detects a special stop subject as described above, A1802 will reject the request if the Special Stops Unit has not reviewed the transaction. When this rejection occurs, ITN/FBI routes the transaction to the Special Stops Unit for review and processing. III/FBI will also send an N3124 when filtering detects an SPF of '5' for a destination outside of IAFIS via the NCIC telecom network. After review, the A1040 may be resubmitted.

(2) III/FBI returns the Criminal History Request Response (A1042) to ITN/FBI or NICS (whichever was the requesting segment). If A1040 requested a displayed response, A1042 will contain the requested information including, for an IDRR, NFF state indicators, if applicable, but not NFF information. If A1040 requested a printed response, A1042 will not contain the requested information but will indicate an acknowledgment of the request and will indicate, for an IDRR, whether NFF data is available.

(3) If A1040 requested a printed IDRR and if the subject record contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message via NCIC to those states.

(4) The state data is returned in the Nlets CR Response (L1048). Otherwise, this step is omitted.

(5) If a printed response was requested, III/FBI will either print the response on the III/FBI high-speed printer,

-or-

(6) III/FBI will send an Unsolicited Report (A3150) message (IDRR/NIDR/Record Set/RANR) for printing on an ITN/FBI or NICS printer.

The following is a list of unsolicited reports that may be requested by the Special Stops Unit and will be sent to ITN/FBI or NICS in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI or NICS.

Report Title	Destination Printer
IDRR/NIDR/ Record Set/RANR	Special Stops
IDRR	NICS

The following is a list of messages which may be spawned from the processing of an Internal Criminal History Request. The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 21.4-03 External Subject Search Data Flow Sequencing and Notes

This DFD applies to the STOTs QH and QWI. This diagram illustrates IAFIS processing of the following types of searches: with FBI Number, without FBI Number, QWI, and Identification for Firearms Sales (IFFS). The QWI has been separated from other subject searches because it has a different Message Key (MKE) and may include search fields used by NCIC for the QW query.

A check for Want or Flash data is made whenever the inquiry contains an FBI Number.

(1) III receives either the III Subject Search Request-QH (N1035) or the Combined NCIC QW and III/FBI-QH Query (QWI) (N1039) message via NCIC when an NCIC user wants;

a) to perform a criminal subject search, or

b) to perform an NCIC Want Inquiry.

(2) III/FBI generates the Subject Search Request Response—QH (N1036) message for either of the above-referenced incoming messages and sends it to the requestor via NCIC.

(3) The following is a list of unsolicited reports that may be spawned from processing an External Criminal History Request and sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on desktop printers in ITN/FBI.

Report Title	Destination Printer
III Participant—Multiple FNUs for III Staff Printer One III-STATE-POINTER	III Staff Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
III Participant QH/QR/ZI/ZR/ ZRS/QWI Response – FBI Research and Advise	III Staff Printer

The following is a list of unsolicited messages which may be spawned from processing an External Subject Search. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 21.4-04 Internal Subject Search Data Flow Sequencing and Notes

This DFD applies to the STOTs SPSS, SSRM, and FASS. This diagram illustrates IAFIS processing of the Internal Subject Search. Internal Subject Searches (SPSS) may be initiated by an IAFIS or NICS Service Provider.

This flow represents either MRD I/O or the interaction of the ITN/FBI with the DPS Service Provider when processing a subject search request.

Service Provider ONLY: The Service Provider makes the request and receives a displayed response on the workstation.

MRD ONLY: If MRD input is unreadable or unacceptable due to improper format or insufficient data, III/FBI writes an MRD Reject response to the tape. MRD response data is both written to tape and mailed to the submitter as hardcopy.

(1) Service Provider ONLY: ITN/FBI or NICS sends a Service Provider Subject Search Request (A1032) message to III/FBI. III/FBI will perform a name search if descriptive data is present in the request. If the A1032 contains a single FNU, an SID or a single SOC, the subject record will be retrieved directly. The inclusion of any descriptors (beyond SID only or a single instance of SOC) will initiate a name search. Refer to the A1032 message definition and the A1032 Processing Matrix below.

Service Provider & MRD: III/FBI performs the subject search or retrieval and performs filtering as required (see IAFIS Filtering Matrix).

(2) Service Provider ONLY: If zero or more than one candidate is returned to ITN/FBI or NICS or if A1032 contained a value of 'Y' in CAND-LIST-FLAG, III/FBI will return a Service Provider Subject Search Candidate List (A1029) message that contains descriptive data for each candidate (if not zero). The Service Provider will then submit another A1032 message containing the FBI number of the candidate selected from the list.

(3) If a single candidate is returned to ITN/FBI or NICS and if A1032 contained a value of 'N' in CAND-LIST-FLAG, III/FBI will generate a Service Provider Subject Search Candidate Record (A1033) message, which contains the record set for that subject, for workstation display. Refer to the A1032 Processing Matrix below for details of Subject Search Response handling.

MRD ONLY: III/FBI writes results to MRD media.

(4) Service Provider & MRD: The following is a list of unsolicited reports that may be spawned from processing an Internal Subject Search and sent to ITN/FBI in the Unsolicited Report (A3150) message. These reports will be formatted by III/FBI and printed on a desktop printer in ITN/FBI .

Report Title	Destination Printer
III Unauthorized Access(UAA) Notification Message	Special Stops Unit
EBTS or Internal Online Printer Response—Hit Against 5, 6, C, K, N, DOD, Missing Person, Unknown Deceased, Amnesia Victim, or Wanted or AUD T Subject	Special Stops Unit (SPF 5, 6, C, N, or AUD of P) Document Specialist (K or DOD) Answer Hits to Wants (SPF I, L or T)

Service Provider & MRD: The following is a list of messages which may be spawned from the processing of an Internal Subject Search. The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

A1032 Processing Matrix						
FNU Retrieval—DFD 21.4-04						
A1032 Contents						III/FBI RESPONSE
STOT	FNU	SOCs	SIDs	SUBJ-SRCH-DATA	CAND-LIST-FLAG	
Any	1-6	0	0	No	N	• If a single FNU is provided and has SCH data (AUD Blank, A, C, E, M, P, T, or W), A1033 w/ the Record Set for the supplied FNU. • If a single FNU is provided, is valid & AUD U is not used, A1033 containing an empty record set with AUD='U' for the supplied FNU. • If multiple FNUs are provided and are valid, A1029 w/ LDSSRs for each FNU • If any FNU is invalid, A1802.
Any	1-6	0	0	No	Y	• If FNU(s) has (have) SCH data, A1029 w/ LDSSR for each FNU. • If any FNU is valid & has no SCH data, A1029 contains provided FNU(s) and AUD='U' • If any FNU is invalid, A1802.
Note: If any FNUs supplied in the A1032 were "killed" in a prior consolidation (AUD = C), the FNU and Record Set returned will be for the "kept" FNU.						

A1032 Processing Matrix						
FNU Retrieval—DFD 21.4-04						
A1032 Contents						III/FBI RESPONSE
STOT	FNU	SOCs	SIDs	SUBJ-SRCH-DATA	CAND-LIST-FLAG	
No subject search is performed under FNU Retrieval						

A1032 Processing Matrix						
SOC Retrieval—DFD 21.4-04						
A1032 Contents						III/FBI RESPONSE
STOT	FNU	SOCs	SIDs	SUBJ-SRCH-DATA	CAND-LIST-FLAG	
Any	0	1	0	No	N	• If 1 subject w/ SOC in SCH, A1033 w/ FNU Record Set. • If more than 1 subject w/ SOC in SCH, A1029 w/ LDSSR for each subject. • If no subject w/ SOC in SCH, A1029 w/ no LDSSR. • If SOC is invalid, A1802. This case does not include an SOC conforming to validation rules that is unassigned.
Any	0	1	0	No	Y	• Same as previous except insert A1029 w/ 1 LDSSR for the A1033 w/ Record Set
Note: Any combination of a SOC and SUBJ-SRCH-DATA (to include additional SOCs) will be treated as a name search.						

A1032 Processing Matrix						
SID Retrieval—DFD 21.4-04						
A1032 Contents						III/FBI RESPONSE
STOT	FNU	SOCs	SIDs	SUBJ-SRCH-DATA	CAND-LIST-FLAG	
Any	0	0	1	No	N	• If 1 subject w/ SID in SCH, A1033 w/Record Set containing matching SID. • If more than 1 subject w/ SID in SCH, A1029 w/ LDSSR for each subject. • If no subject w/ SID in SCH, A1029 w/ no LDSSR. • If SID is invalid, A1802. This case does not include a SID conforming to validation rules that is unassigned.
Any	0	0	1	No	Y	• Same as previous except insert A1029 w/ 1 LDSSR for the A1033 w/ Record Set
Note: Any combination of a SID and SUBJ-SRCH-DATA will be treated as a name search.						

A1032 Processing Matrix						
Subject Search Only—DFD 21.4-04						
A1032 Contents						**III/FBI RESPONSE**
STOT	**FNU**	**SOCs**	**SIDs**	**SUBJ-SRCH-DATA**	**CAND-LIST-FLAG**	
Any	0	0	0	No	N or Y	• ITN/FBI S/W prevents such a submission.
Any	0	0	0	Yes	N	• If 1 candidate from subject search, A1033 w/ Record Set for candidate. • If more than 1 candidate from subject search, A1029 w/ an LDSSR for each candidate. • If no candidates from subject search, A1029 w/ no LDSSR.
Any	0	0	0	Yes	Y	• Same as previous except insert A1029 w/ 1 LDSSR for each A1033 w/ Record Set.

Figure 21.4-05 External III/FBI Administrative Inquiry (ZI) Data Flow Sequencing and Notes

This DFD applies to the STOT ZI. This diagram illustrates IAFIS processing of a III/FBI Administrative Inquiry. The ZI query is used by III participants when there is a need to determine:

a) the presence of a SID or FBI pointer and the date established;

b) single-, multi-state or wanted status;

c) dates of establishment and/or last update.

(1) The III Administrative Inquiry-ZI Inquiry (N3050) message is received by IAFIS via NCIC.

(2) III/FBI processes the request and returns the III Administrative Response—ZI (N3051) message and sends it to the inquiring agency via NCIC.

(3) The Unsolicited Report (A3150) message may be spawned from processing an External III/FBI Administrative Inquiry. This report will be formatted by III/FBI and printed on desktop printer in ITN/FBI.

Report Title	Destination Printer
III Participant—Multiple FNUs for One III-STATE-POINTER	III Staff Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit

The following is a list of unsolicited messages which may be spawned from processing an External III/FBI Administrative Inquiry. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 21.4-06 External III/FBI Record Availability Inquiry (ZR) Data Flow Sequencing and Notes

This DFD applies to the STOT ZR. This data flow illustrates IAFIS processing of a III Availability Inquiry. The ZR query is used to determine, by providing an FBI or SID number, if a subject record is on file in the III.

(1) The III Record Availability Inquiry-ZR (N3052) message is received by IAFIS via NCIC.

(2) III/FBI processes the request and returns the III Record Availability Response—ZR (N3053) message and sends it to the inquiring agency via NCIC.

(3) The Unsolicited Report (A3150) message may be spawned from processing an External III/FBI Administrative Inquiry. This report will be formatted by III/FBI and printed on a desktop printer in ITN/FBI.

Report Title	Destination Printer
III Participant—Multiple FNUs for One III-STATE-POINTER	III Staff Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit

The following is a list of unsolicited messages which may be spawned from processing an External III/FBI Record Availability Inquiry. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 21.4-07 External III/FBI Record Status Inquiry (ZRS) Data Flow Sequencing and Notes

This DFD applies to the STOT ZRS. This data flow illustrates IAFIS processing of a III/FBI Record Status Inquiry. The ZRS query is used when a III participant wants to verify the status, single- or multi-state, of a subject record.

(1) The III Record Status Inquiry-ZRS (N3054) message is received by IAFIS via NCIC.

(2) III/FBI processes the request and returns the III Record Status Response—ZRS (N3055) message and sends it to the inquiring agency via NCIC.

(3) The Unsolicited Report (A3150) message may have spawned from processing an External III/FBI Administrative Inquiry. This report will be formatted by III/FBI and printed on desktop printer in ITN/FBI.

Report Title	Destination Printer
III Participant—Multiple FNUs for One III-STATE-POINTER	III Staff Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit

The following is a list of unsolicited messages which may spawn from processing an External III/FBI Record Status Inquiry. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3112 (MSO) Multi-state Offender Status
N3121 (SSO) Single State Offender Status Notification
N3124 Unsolicited Activity Notification

Figure 21.4-08 Ad Hoc Subject Search Data Flow Sequencing and Notes

This DFD applies to the STOT AHSS. This data flow illustrates IAFIS processing of an Ad Hoc Subject Search Request. The Ad Hoc Subject Search is an internal process initiated from an ITN/FBI workstation. It is designed to provide capability for searches of both the Subject Criminal History File and the Civil Subject Index Master File held in III/FBI. This process is not available through any other IAFIS transaction. This flow represents the interaction between the ITN/FBI Service Provider or OFO workstation and IAFIS. The request is initiated and the response is displayed at the workstation.

(1) The Ad Hoc Subject Search Request—String (A1132) message contains the Ad Hoc search parameters, the file to be searched (criminal or civil, one file per request), whether the results are to be returned as a file, and the maximum number of candidates to be returned. The Ad Hoc Subject Search HMI contains a check box that allows the operator to specify that only subjects whose records have associated images (based on AUD code) be returned as candidates. When checked, ITN/FBI will automatically include an AUD code restriction in the query. This feature will provide Latent Specialists with the ability to populate a Special Latent Cognizant (SLC) file, insuring that no attempt will be made to add a subject whose record contains no images; out-of-synch conditions will initiate error processing.

(2) III/FBI performs the search and returns the Ad Hoc Subject Search Response (A1133) message with the following result:

a) If the value of 'DOFILE' in the request was 'N,' only a count of the records matching the search criteria will be returned and displayed, and the process is ended.

b) If the search was performed against the Criminal Master File and the value of 'DOFILE' in the request was 'Y,' ITN/FBI will, upon the return of A1133, use the FNUs provided by III/FBI to retrieve descriptive data for the matching records. This will occur in the background via the number of instances of A1032/A1029 required to retrieve the descriptive data up to the limit of 240 candidates. For these background instances of A1032 initiated as the result of an Ad Hoc query, the value of CAND-LIST-FLAG will always be set to 'Y.'

i) The service provider may then elect to request the record set for a single candidate chosen from the list(s) presented. ITN/FBI will use A1032/A1033 for this retrieval.

NOTE: Refer to DFD 21.4-04 Sequencing and Notes for further detail regarding the conditions and use of messages A1032, A1029, and A1033.

ii) The latent service provider has the option of either copying the images for the entire list of candidates to a specified SLC file, copying the images for selected candidates to a selected SLC file, or retrieving the images for candidates from the list to be added to the image log (refer to DFD 21.5-18).

c) If the search was performed against the Civil Subject Master File and the value of 'DOFILE' in the request was 'Y,' ITN/FBI will, upon the return of A1133, use the CRNs provided by III/FBI to retrieve descriptive data for the matching records. This will occur in the background via the number of instances of A1061/A1059 required to retrieve the descriptive data up to the limit of 240 candidates. For these background instances of A1061 initiated as the result of an Ad Hoc query, the value of CAND-LIST-FLAG will always be set to 'Y'.

i) The service provider may then elect to request the record set for a single candidate chosen from the list(s) presented. ITN/FBI will use A1061/A1060 for this retrieval.

NOTE: Refer to DFD 21.1-09 Sequencing and Notes for further detail regarding the conditions and use of messages A1059, A1060, and A1061.

ii) The latent service provider has the option of either copying the images for the entire list of candidates to a specified SLC file, copying the images for selected candidates to a selected SLC file, or retrieving the images for candidates from the list to be added to the image log (refer to DFD 21.5-18).

If the request contained a value of 'Y' in field 'DOFILE,' A1133 will populate the field 'FILEHANDLE' containing the name of and the path to the Ad Hoc Subject Search Results File Format (I3022). III/FBI will write this file to the specified location within ITN/FBI.

Figure 21.4-09 Electronic Identity History Request Data Flow Sequencing and Notes

This diagram applies to the STOT EIHR, and illustrates the messaging sequence used when an external agency submits a bulk softcopy request for criminal histories.

When the FBI receives a bulk softcopy request from an external agency, EFCON/FBI will format one E1047 message per FNU.

(1) EFCON/FBI will send the E1047 to ITN/FBI, who will convert it to an A1047 and set PUR='C'.

(2) ITN/FBI sends the A1047 to III/FBI.

NOTE: III/FBI performs filtering for Special Stop subjects (SPF = '5' or '6' or 'C' or 'N'). III/FBI will send an N3124 when filtering detects an SPF of '5' or '6' for a destination outside of IAFIS via the NCIC telecom network. Transaction Response Types (TRT) will be sent for each successful EIHR.

(3) III/FBI will reply to ITN/FBI with an A1049 message to acknowledge receipt of the A1047.

(4) III/FBI will, if necessary, send an Unsolicited Criminal History Request (N3105) via NCIC to any state with an active NFF pointer on the record.

(5) The state data is returned in the Nlets CR Response (L1048)

(6) III/FBI will consolidate the NFF responses, build the A1080 message, and send it to ITN/FBI.

(7) ITN/FBI will remove the IAFIS header and forward the resulting the E1080 message to EFCON who will gather all responses and write them to electronic media for the requesting agency.

The following is a list of messages which may be spawned from the processing of an Electronic Identity History Request. The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name	
N3124	Unsolicited Activity Notification

Figure 21.5-01 Remote Latent Search Data Flow Sequencing and Notes

This DFD applies to the STOTs LFFS and LFIS. This diagram illustrates IAFIS processing of a Remote Latent Search. The following types of transactions are included in this data flow: LFIS and LFFS.

(1) A Remote Latent Search Request (E1021) message is received by IAFIS via the CJIS WAN. ITN/FBI will write this EBTS message to disk and send to AFIS/FBI a Remote Latent Search (A1021) message containing the Header and 'FILEHANDLE,' which AFIS/FBI uses to retrieve the image file from ITN/FBI. The image file is formatted per I1021.

(2) AFIS/FBI will perform the latent search of the CMF and generate the Remote Search Candidate List (A1034) message to III/FBI. The A1034 will indicate that the latent record(s) will be added to the ULF, if the ULF flag in the E1021 contained a value of 'Y,' and will include the resultant ULF index number.

(3) When III/FBI receives the A1034, it will perform filtering of the candidate list and, if necessary, send a Review Request (A1312) message to ITN/FBI.

(4) If III/FBI filtering spawned a Review Request, ITN/FBI will respond with the Review Response (A1313) message.

(5) III/FBI will send an Internal Fingerprint Image Request (A1053) message to ITN/FBI for the candidates for which the originator requested images and whose records contain an AUD = 'BLANK,' or 'N.'

(6) ITN/FBI will retrieve and hold the requested images and return the Internal Fingerprint Image Response (A1054) message to III/FBI.

(7) III/FBI will return the candidate list information from the Subject Criminal History File, construct the Remote Latent Search Response (A1024) message in EBTS format, and send it to ITN/FBI. ITN/FBI will append the images and send the resulting Remote Latent Search Response (E1024) message to the external user via the CJIS WAN.

(8) After AFIS/FBI completes the search of the CMF, the Unsolved Latent Image Add (A3301) message is sent to ITN/FBI for every I1021 file received. The A3301 contains the 'FILEHANDLE' passed to AFIS/FBI in the A1021 message and is used to notify ITN/FBI that the original image file (I1021) can now be deleted. If the latent has been added to the ULF at AFIS/FBI and a ULF image is available, the A3301 will have the ULF image's present flag set to 'Y' to tell ITN/FBI to retain the latent image(s) in the ULF.

(9) If the E1021 message contains a request to add the search latent fingerprint(s) to the Unsolved Latent File and the File/Subfile contains the maximum number of allowable records, AFIS/FBI will delete the oldest record in the Unsolved Latent Features File and, if the record has a corresponding image in the Unsolved Latent Image File, will send an Unsolved Latent Image Delete (A3326) message to ITN/FBI.

(10) AFIS/FBI will send an unsolicited Unsolved Latent Delete Notice (A3341) message to the owner of the deleted latent record. An STOT of UULD will be assigned to this process. AFIS/FBI will use the ORI of the record owner to determine whether to send the message to ITN/FBI for Internally owned records or to III/FBI for records owned by external users. If externally owned, III/FBI will receive the A3341 and send an Unsolicited Unsolved Latent Delete Notice (External) (A3342) message to ITN/FBI. ITN/FBI will convert the message into an External Unsolicited Unsolved Latent Delete (E3342) and forward the message to EFCON/FBI which will send it to the external user via the CJIS WAN.

NOTE: If an Unsolved Latent File add is not confirmed within 9999 days (27

years), the record will be deleted.

Figure 21.5-02 External Latent Submission Data Flow Sequencing and Notes

This data flow applies to the STOTs ELR, LFS, CFS, and MCS. This diagram illustrates IAFIS processing of an External Latent Submission.

(1) The External Latent Submission (E1010) message will be received by IAFIS via the CJIS WAN.

(2) An FBI FAS Latent Specialist may initiate a Service Provider Subject Search Request (A1032) message to III/FBI as part of submission processing. This message may contain an FBI number and, optionally, descriptive search data. III/FBI will perform a name search if descriptive data is present in the request. If both FNU and descriptive data are included, III/FBI will retrieve the record for the supplied FNU and provide candidates resulting from the name search.

NOTE: If the requester is an Other Federal Organization (OFO) User (as determined by AUTH Code), III/FBI will only return candidates whose records contain an AUD value that is equal to either 'BLANK' or 'M.'

(3) Note that two possible messages can occur in this step and will be produced according to the following conditions:

If zero or more than one candidate is to be returned to ITN/FBI, III/FBI will return the Service Provider Subject Search Candidate List (A1029) message that contains descriptive data for each candidate (if not zero);

When A1032 contains a value of 'Y' in CAND-LIST-FLAG, the response will always be A1029;

If CAND-LIST-FLAG = 'N' and a single candidate is to be returned to ITN/FBI, III/FBI will return the Service Provider Subject Search Candidate Record (A1033) message that contains the criminal history data for that subject.

NOTE: Refer to DFD 21.4-04 Sequencing and Notes for further detail regarding the conditions and use of messages A1032, A1029, and A1033.

(4) An FBI FAS Latent Specialist in ITN/FBI may initiate an AFIS Ten-Print Search (A1027) message to AFIS/FBI, searching the Criminal Master File, the Civil On-line Features File, or a Special Latent Cognizant File (determined by the value of NDR). A1027 contains the FILEHANDLE which AFIS/FBI will use to retrieve the file containing images from ITN/FBI. The file is formatted in accordance with I3020.

(5) AFIS/FBI will return the AFIS Search Response Data Candidate List (A1022) message containing a list of candidate subjects by UCN accompanied by the search score. There may be zero candidates.

(6) To present limited subject information with each candidate image resulting from the AFIS/FBI search and sent to the FAS Specialist, ITN/FBI will prestage the information by sending A1032 for criminal candidates and a Civil Subject Retrieval (A1061) for civil candidates, providing an FNU or CRN and a value of 'Y' in CAND-LIST-FLAG, to III/FBI. If the requester is an OFO (as determined by AUTH Code), III/FBI will only return candidates whose records contain an AUD value that is equal to either 'BLANK' or 'M.'

(7) III/FBI returns a Service Provider Subject Search Candidate List (A1029) for criminal candidates and a Civil Candidate List (A1059) for civil candidates to ITN/FBI. If A1029 indicates a Special Stop subject was detected, ITN/FBI will route only the stopped subject to the Special Stops Unit. ITN/FBI will retrieve candidate images from the ISRE and will allow the FBI FAS Latent Specialist to view the remaining FNUs. ITN/FBI will inform the FBI FAS Latent Specialist that the image for the stopped FNU is unavailable,

and will maintain the unavailable FNU in the proper ranked position in the candidate list as displayed to the FBI latent specialist. The FBI FAS Latent Specialist will call the Special Stops Unit to determine further processing of the stopped FNU. If the requester is an OFO (as determined by AUTH Code), ITN/FBI- Special Stops will remove the candidate from the list displayed to the OFO user. The OFO user is not notified of this removal.

(8) An FBI FAS Latent Specialist may initiate a features search of either the Criminal Master File, the Civil Online Features File, or the Special Latent Cognizant Files using the Internal Latent Features Search (A1028) message to AFIS/FBI. This message may include a request to add the features as a record in the Unsolved Latent File (ULF).

(9) AFIS/FBI will then send a Latent Feature Search Candidate List (A1016) message to ITN/FBI. If the ULF Add was requested (ULF = 'Y') the ULF index will be returned in the A1016.

NOTE: Candidate information is returned as the same manner in as paragraphs 6 and 7.

(10) The FBI FAS Latent Specialist will process the submission based on the results of the searches and ITN/FBI will send a Latent Submission Response Data (A1012) message to III/FBI in response to a TOT of LFS, or

If filtering (of A1012) reveals a Special Stop subject, an A1802 will reject A1012 for Unauthorized Access. When this rejection occurs, ITN/FBI will route the transaction to Special Stops for review. Upon completion of the review, ITN/FBI resends A1012.

(11) ITN/FBI will send a Latent Submission Response Data Notification of Action (A1014) message in response to a TOT of ELR.

(12) If a subject record (in an Idented submission) will be provided and contains active NFF state pointers, III/FBI may send an Unsolicited Criminal History Request (N3105) message to those states.

(13) The states return their data in the Nlets CR Response (L1048) message.

III/FBI will assemble the appropriate data and:

(14) build the Latent Submission Response (A1013) message and send it to ITN/FBI. (processing will continue with paragraph 14) or;

(15) Latent Submission Response—Notification of Action (A1015) message in EBTS format and send it to ITN/FBI (processing will continue with paragraph 15).

ITN/FBI will convert the message and:

(16) Append the Type-4 record(s) (images) and send the resulting External Latent Submission Response (E1013) message, or

(17) Send the External Latent Submission—Notification of Action (E1015) message;

and send the message to EFCON/FBI which will forward the message to the submitter via the CJIS WAN.

(18) If the latent submitter requested the response be sent to other agencies that are not electronic-capable, III/FBI will print responses.

(19) If the message included a request to add a record to the ULF and the file/subfile contains the maximum number of allowable records, AFIS/FBI will delete the oldest record in the subfile and send an Unsolved Latent Image

Delete (A3326) message to ITN/FBI.

(20) AFIS/FBI will send an unsolicited Unsolved Latent Delete Notice (A3341) message to the owner of the deleted latent record. An STOT of UULD will be assigned to this process. AFIS/FBI will use the ORI of the record owner to determine whether to send the message to ITN/FBI for Internal Users' FAS/OFO-owned records or to III/FBI for records owned by external users.

(21)If externally owned, III/FBI will receive the A3341 and will send an Unsolicited Unsolved Latent Delete Notice (External) (A3342) message to ITN/FBI. ITN/FBI will remove the IAFIS Header and forward the resulting External Unsolicited Unsolved Latent Delete (E3342) message to the external user via the CJIS WAN.

(22) If the latent record is added to the ULF at AFIS/FBI, AFIS will send the Unsolved Latent Image Add (A3301) message to ITN/FBI. ITN/FBI will add the corresponding image to the Unsolved Latent Image File.

Figure 21.5-03 Internal Latent Submission Data Flow Sequencing and Notes

This DFD applies to the STOT ILFS. This diagram illustrates IAFIS processing of an internal latent submission. With the exception of the input via the CJIS WAN, the sequencing and notes for this Data Flow Diagram are the same as for 21.5-02 for message flows #1—9. This data flow begins with a hardcopy input entered via the Latent Processing Workstation (part of FBI FAS Latent Specialist in ITN/FBI) and not the E1010 (1) as shown in 21.5-02.

NOTE: If the latent specialist makes an Ident, and the subject record is to be provided, ITN/FBI sends a Criminal History Request as described in DFD 21.4-02.

(10) If the submission includes a request to add the search latent fingerprint(s) to the Unsolved Latent File and the File/Subfile contains the maximum number of allowable records, AFIS/FBI will delete the oldest record in the Unsolved Latent Features File and, if the record has a corresponding image in the Unsolved Latent Image File, will send an Unsolved Latent Image Delete (A3326) message to ITN/FBI.

(11) AFIS/FBI will send an unsolicited Unsolved Latent Delete Notice (A3341) message to the owner of the deleted latent record. An STOT of UULD will be assigned to this process. AFIS/FBI will use the ORI of the record owner to determine whether the image is internally or externally owned. If the Image is externally owned, the A3341 will be sent to III/FBI for records owned by external users. III/FBI will receive the A3341 and send an Unsolicited Unsolved Latent Delete Notice (External) (A3342) message to ITN/FBI. ITN/FBI will convert the message to an External Unsolicited Unsolved Latent Delete (E3342) message and forward it to EFCON/FBI which will send the message to the external user via the CJIS WAN.

(12) If the ULF image is internally owned (as determined by the ORI), AFIS/FBI will send the A3341 to ITN/FBI.

(13) If the latent record is added to the ULF at AFIS/FBI, AFIS will send the Unsolved Latent Image Add (A3301) message to ITN/FBI. ITN/FBI will add the corresponding image to the Unsolved Latent Image File.

Figure 21.5-04 Internal Unsolved Latent Search Data Flow Sequencing and Notes

This DFD applies to the STOTs IULS and IULTS. This diagram illustrates the processing of an internal latent search as requested by a Latent Specialist from an ITN/FBI workstation.

This flow represents the interaction as a Latent Specialist scans and submits an image (Ten-print or latent) for searching and views the result.

(1) If the image to be searched is a latent, ITN/FBI sends the LPS ULF Latent Search (A1017) to AFIS/FBI.

-or-

(1) If the image to be searched is a Ten-print, ITN/FBI sends the LPS ULF Ten-print Search (A1018) to AFIS/FBI. The A1018 contains the filehandle which AFIS/FBI uses to retrieve the image file from ITN/FBI. The file is formatted in accordance with I3020.

(2) AFIS/FBI returns the LPS ULF Search Response (A1019) containing the results of the Unsolved Latent File search to the Latent Specialist.

Figure 21.5-05 Internal Unsolved Latent Delete Data Flow Sequencing and Notes

This data flow applies to the STOT IULD. This diagram illustrates the process of deletion of an image from the Unsolved Latent File. The transaction is initiated by a Latent Specialist at a local workstation. This flow represents the interaction of ITN/FBI with the Latent Specialist as the processing activity occurs. The Latent Specialist initiates the deletion by providing information identifying the latent image to be removed.

(1) ITN/FBI sends the Internal Unsolved Latent Delete Request (A3322) message to AFIS/FBI.

(2) AFIS/FBI performs the requested delete by removing the features record and sends the Unsolved Latent Image Delete (A3326) message to ITN/FBI requesting deletion of the corresponding image.

(3) AFIS/FBI notifies ITN/FBI of completion of the delete by sending the Delete Unsolved Latent Record Response (A3328). The results of this record removal are displayed to the Latent Specialist at the workstation.

Figure 21.5-06 External Unsolved Latent Delete Data Flow Sequencing and Notes

This DFD applies to the STOT ULD. This diagram illustrates the process of deletion of an image from the Unsolved Latent File by a remote user. The transaction is initiated by EBTS-compliant messaging received by IAFIS via the CJIS WAN.

(1) IAFIS receives the External Unsolved Latent Delete (ULD) (E3325) message via the CJIS WAN. ITN/FBI prepares the Delete Unsolved Latent Record Request (External) (A3325) message and sends it to AFIS/FBI.

(2) AFIS/FBI performs the requested delete by removing the features record and sends the Unsolved Latent Image Delete (A3326) message to ITN/FBI requesting deletion of the corresponding image.

(3) AFIS/FBI sends III/FBI the Delete Unsolved Latent Record Response (A3328).

(4) III/FBI prepares the Unsolved Latent Delete Response (External) (A3329) according to the EBTS and sends it to ITN/FBI. ITN/FBI converts the message to an E3329 and forwards it to EFCON/FBI which will send the E3329 message to the contributor via the CJIS-WAN.

Figure 21.5-07 Internal Unsolved Latent Add Confirm Data Flow Sequencing and Notes

This DFD applies to the STOT IULAC. This diagram illustrates the process of the confirmation of an image add to the Unsolved Latent File. The transaction is initiated by a Latent Specialist at a local workstation.

(1) The Latent Specialist initiates the add/confirm by providing information identifying the latent image, the addition of which is to be confirmed. ITN/FBI sends the Internal Unsolved Latent Add Confirm (A3354) message to AFIS/FBI.

(2) AFIS/FBI performs the requested action and sends the Unsolved Latent Add Confirm (A3352) message to ITN/FBI containing identifiers for the record confirmed. The results of this action are displayed to the Latent Specialist at the workstation.

Figure 21.5-08 External Unsolved Latent Add Confirm Data Flow Sequencing and Notes

This DFD applies to the STOT ULAC. This diagram illustrates the process of the confirmation of an image add to the Unsolved Latent File by a remote user. The transaction is initiated by EBTS-compliant messaging received by IAFIS via the CJIS WAN.

(1) IAFIS receives the External Unsolved Latent Add Confirm (E3351) message via the CJIS WAN. ITN/FBI prepares the Unsolved Latent Add Confirm (External) (A3351) message and sends it to AFIS/FBI.

(2) AFIS/FBI performs the requested add/confirm and sends the Unsolved Latent Add Confirm Response (A3352) message to III/FBI.

(3) III/FBI prepares the Unsolved Latent Add Confirm Response (External) (A3353) according to the EBTS and sends it to ITN/FBI. ITN/FBI converts the message to an External Unsolved Latent Add Confirm (E3353) and forwards it to EFCON which will send the message to the contributor via the CJIS WAN.

Figure 21.5-10 Internal Latent Search Penetration Query Data Flow Sequencing and Notes

This DFD applies to the STOT ILPNQ. This diagram illustrates IAFIS processing of the Internal Latent Search Penetration Query. A penetration query is submitted before submitting a Latent Search to assure that search penetration does not exceed thirty percent of the Criminal Master File. This flow represents the interaction of the Latent Specialist as the penetration query activity occurs.

(1) The specialist initiates the request, including a set of descriptive data. ITN/FBI will send an Internal Latent Search Penetration Query (A3070) message to AFIS/FBI. AFIS/FBI will perform the processing needed to determine percent of penetration, based on the particular set of descriptive data received in the A3070, into the Criminal Master File.

(2) AFIS will accept A3070 & respond with A1802 containing error code L0016 to report search penetration.

Figure 21.5-11 Latent External Search Penetration Query Data Flow Sequencing and Notes

This DFD applies to the STOT LPNQ. This diagram illustrates IAFIS processing of an External Latent Search Penetration Query. A penetration query is required before submitting a Latent Search to assure that search penetration does not exceed thirty percent of the Criminal Master File.

(1) A Latent Search Penetration Query (E3061) message is received by IAFIS via the CJIS WAN. ITN/FBI will attach an IAFIS header to the message and send the resulting Latent Search Penetration Query (A3061) message to AFIS/FBI for processing.

(2) AFIS/FBI will calculate the percentage of penetration for the given parameters in the query and forward the Latent Penetration Query Response Data (A3067) message to III/FBI.

(3) III/FBI will format the response data in accordance with the EBTS and send the resulting Latent Penetration Query Response (A3062) message to ITN/FBI. ITN/FBI will convert the message to a Latent Penetration Query Response (E3062) message which is forwarded to EFCON which will send the message to the contributor via the CJIS-WAN.

Figure 21.5-13 Latent Repository Statistics Query Data Flow Sequencing and Notes

This DFD applies to the STOT LRSQ. This diagram illustrates IAFIS processing of a Latent Repository Statistics Query. This query provides a statistical representation, based on descriptive data, of a latent repository and is used in updating a user's statistical representation to be used in a penetration query.

(1) IAFIS will receive the Latent Repository Statistics Query (E3063) message via the CJIS WAN. ITN/FBI will prepare the resulting Latent Repository Statistics Query (A3063) message and send it to AFIS/FBI for processing.

(2) AFIS/FBI will process the input and produce a Latent Repository Statistics Response Data (A3068) message containing a statistical representation of the descriptors in the Latent Cognizant File and send it to III/FBI.

(3) III/FBI will format the message in accordance with the EBTS and send the resulting Latent Repository Statistics Response (A3064) message to ITN/FBI. ITN/FBI will convert the message to a Latent Repository Statistics Response (E3064) message and forward it to EFCON which will send the message to the contributor via the CJIS WAN.

Figure 21.5-14 Internal Latent Search Status and Modification Query Data Flow Sequencing and Notes

This DFD applies to the STOT ILSMQ. This diagram illustrates IAFIS processing of an Internal Latent Search Status and Modification Query. This is used to determine the status of a submitted latent search and, optionally, to modify that status. This flow represents the interaction of the Latent Specialist as the Search Status and Modification activity occurs.

(1) The specialist initiates the request and is provided with a response on the workstation display. ITN/FBI will send the Internal Latent Search Status and Modification Query (A3072) message to AFIS/FBI for processing.

(2) AFIS/FBI will process the query and return an Internal Latent Search Status and Modification Response (A3073) message to ITN/FBI. The response is routed, to the Latent Specialist

Figure 21.5-15 External Latent Search Status and Modification Query Data Flow Sequencing and Notes

This DFD applies to the STOT LSMQ. This diagram illustrates IAFIS processing of a Latent Search Status and Modification Query. External users may submit a query to discover the status of a submitted search and, optionally, to modify that status

(1) IAFIS will receive the Latent Search Status and Modification Query (E3065) message via the CJIS WAN. ITN/FBI will attach an IAFIS header and forward the resulting Latent Search Status and Modification Query (A3065) message to AFIS/FBI for processing.

(2) AFIS/FBI will process the query and send a Latent Search Status and Modification Response Data (A3069) message to III/FBI.

(3) III/FBI will format the message in accordance with the EBTS and send the resulting Latent Search Status and Modification Response (A3066) message to ITN/FBI. ITN/FBI will convert the message to a Latent Search Status and Modification Response (E3066) and forward it to EFCON which will send the message to the contributor via the CJIS-WAN.

Figure 21.5-16 Special Internal Latent Cognizant Add or Delete Data Flow Sequencing and Notes

This DFD applies to the STOT ISLC. This diagram illustrates IAFIS processing of record addition and record deletion activity against the Special Latent Cognizant Files. These operations are initiated by a Latent Specialist from an ITN/FBI workstation. This flow represents the interaction of the Latent Specialist as the record add or delete activity occurs.

(1) FBI FAS Latent Specialist only: The specialist initiates an add or delete request—for a Record Add request, the specialist will enter values for UCN and SLC. ITN/FBI will send either the Special Latent Cognizant—Record Add (A1065) or Special Latent Cognizant—Record Delete (A1067) message to AFIS/FBI. A1065 contains the FILEHANDLE which AFIS/FBI will use to retrieve the file containing images from ITN/FBI. The file is formatted in accordance with I3020.

(2) AFIS/FBI will perform the requested operation and return the Special Latent Cognizant—Record Maintenance Response (A1066) message to ITN/FBI. NDR in A1066 will indicate the file that was updated. The response is routed, using EID, to the Latent Specialist via e-mail.

Figure 21.5-17 Card Scanning Service Special Latent Cognizant Submission Supplemental Data Flow Sequencing and Notes

This data flow applies to the STOT SLCC. This diagram illustrates the message sequence for those messages specific to processing SLC Add transactions received through the Card Scanning Service (CSS) facility and transmitted to IAFIS via the CJIS WAN.

(1) ITN/FBI will receive the Electronic Special Latent Cognizant Add (E1011), via EFCON and the CJIS WAN. The E1011 message has a TOT of SLCC and an ORI identifying the origin as CSS. SLC records will be added directly to the SLC file designated by the value of NDR in the E1011 message and will not appear in the Latent Specialist's Submission or Image logs.

(2) If the card data is complete, ITN/FBI will send the Special Latent Cognizant-Record Add (A1065) message to AFIS/FBI.

If front-end validation fails, EFCON sends an E1804.

(3) If ITN/FBI initiates A1801, III/FBI formats an A1804 and sends it to ITN/FBI which converts the message to an E1804. ITN/FBI sends the E1804 to EFCON which will send it to CSS via the CJIS WAN. (Refer to DFD 21.6-01 for error processing detail.) This message notifies the CSS of transaction reject.

NOTE: While error messages are not normally shown on the diagrams, A1801/A1804/E1804 error messages are shown on this DFD to increase understanding.

(4) AFIS/FBI will perform the requested operation and return the Special Latent Cognizant—Record Maintenance Response (A1066) message to ITN/FBI. NDR in A1066 will indicate the file that was updated. ITN/FBI will add the images to the file indicated in the A1066.

Figure 21.5-18 Special Latent Cognizant Record Copy Data Flow Sequencing and Notes

This DFD applies to the STOT ISLC. This diagram illustrates both of the following:

a) the process of copying an entire Special Latent Cognizant (SLC) file, and

b) copying selected records from any AFIS/FBI features file to an SLC file. The transaction is initiated by a Latent Specialist at a workstation.

SLC Copy All

Before a Latent Specialist initiates a transaction to copy an entire SLC to another file using COPY_ALL_SLC, a request to place the source and target files in an offline condition must be communicated to the AFIS/FBI Segment Administrator, typically via phone.

(1) The Latent Specialist initiates the copy transaction by specifying both the source file containing the records to be copied and the newly created destination SLC. ITN/FBI sends the Special Latent Cognizant—Copy (A1069) message to AFIS/FBI.

(2) AFIS/FBI will perform the requested file copy and return the Special Latent Cognizant—Copy Maintenance Response (A1070). The AFIS/FBI Segment Administrator will return the source and target files to an on-line condition.

(3) If the source SLC file specified in the A1069 has not been placed in an offline condition, AFIS/FBI will send an Error Notification (A1802).

SLC Record Copy

(4) A Latent Specialist initiates a copy transaction by specifying the source file, the records to be copied and the destination SLC. ITN/FBI performs the requested copy and sends the Special Latent Cognizant—Copy (A1069) message to AFIS/FBI.

(5) AFIS/FBI will perform the requested file copy and return the Special Latent Cognizant—Copy Maintenance Response (A1070). This message will contain the identifier(s) for any record(s) that were not successfully copied to the target file. The response is displayed at the workstation.

Figure 21.5-19 Unsolicited Post Latent Search Candidate Processing Data Flow Sequencing and Notes

This DFD applies to the STOT UPLP. This diagram illustrates IAFIS processing of the Unsolicited Post Latent Search Processing Candidate. This data flow has been separated from the other diagrams for the sake of clarity.

Latent Searches of the CMF generate extended candidate lists (containing search scores) which are stored in AFIS/FBI for subsequent candidate list correlation to provide additional candidates to the latent service providers. Every internal (A1028) latent search is processed against the data from the latent searches previously stored in the database to determine possible candidate correlations. The identified candidates are populated into the candidate table with their scores. At a pre-determined time interval, a subset of the candidates in the candidate table will be selected to be sent to the latent specialist for further comparison. Each candidate selected will result in a unique Unsolicited Post Latent Processing Candidate Message. The number of latent searches stored in the database and the length of time a search is retained in the database remain configurable parameters.

(1) AFIS/FBI creates the Unsolicited Post Latent Processing Candidate Message (A3345) and sends the message to ITN/FBI.

(2) ITN/FBI adds the candidate to the candidate list information in the original search so it will not duplicate entries. E-mail is sent to the Forensic Analysis Section (FBI FAS) latent specialist as the first notification of a post latent processing candidate. (Note: the e-mail does NOT contain the FNU.) For compliance with Special Stops processing and to present limited subject information for the candidate image resulting from the AFIS/FBI Post Latent Processing Correlation, ITN/FBI pre-stages the information by sending A1032 to III/FBI.

Note: Results of Latent Searches of the CMF initiated by OFOs are stored and A3345s are returned to ITN/FBI if correlations occur. OFOs do NOT have access to the PLP HMI Candidate List and, as a result, this additional information is unavailable to OFO latent operators.

(3) III/FBI returns a Service Provider Subject Search Candidate List (A1029) message to ITN/FBI. If the A1029 indicates a Special Stops subject was detected, ITN/FBI will route the stopped subject to the Special Stops Unit. ITN/FBI will retrieve candidate images from the ISRE and will allow the FAS latent specialist to view the remaining FNUs from the original latent search. ITN/FBI will inform the FAS latent specialist that the image for the stopped FNU is unavailable. The unavailable FNU remains in proper ranked position in the original latent search candidate list as displayed to the FAS latent specialist. The FAS latent specialist will call the Special Stops Unit (using the phone number on the HMI) to request release of the stopped candidate FNU.

Figure 21.6-01 Transaction Error Data Flow Sequencing and Notes

This DFD applies to the STOT ERRA. The Transaction Error Data Flow diagram depicts the message flows that occur when an external message received via the CJIS WAN or an inter-segment transaction results in an error response. The segment detecting the error is responsible for initiating the message flows. Refer to Section 5.10 for additional error message generation and handling information. NCIC message errors cause either a negative acknowledgment (NAK character) or a related NCIC error message generated by III/FBI. NCIC error responses are not shown on this data flow.

(1) If a segment detects invalid data during message acceptance processing or is otherwise unable to accept a message, the segment immediately responds (IR protocol) with an Error Notification (A1802) to the sending segment. If a receiving segment detects an error while performing the service requested in a message, the segment responds with an A1802 using the same protocol (IR or KR) that the service response would have used. Selected service request processing and message validation errors are routed to a Service Provider for review; otherwise the Segment Administrator is notified. Authorized Service Providers may reject an EBTS submission or request for service, optionally providing a reason for rejection or amplifying information to the originator.

(2) If the owner of an EBTS transaction (either ITN/FBI or AFIS/FBI) detects data validation or message format errors in the incoming message, the segment will send an EBTS Error Response Request (A1801) to III/FBI. If a Service Provider rejects the EBTS submission, ITN/FBI will send an A1801 to III/FBI. Up to ten data validation or message format errors and one reason for rejection may be reported in one message.

(3) III/FBI converts the error message codes to operator-intelligible text, then generates and sends the EBTS Error Response (A1804)

(4) ITN/FBI converts the A1804 to an Electronic Error Response (E1804) and forwards it to EFCON which will send the message to the contributor via the CJIS-WAN. (Refer to DFD 21.6-01 for error processing detail.)

Figure 21.7-01 INS/ICE IDENT/IAFIS Rapsheet Request Data Flow Sequencing and Notes

This DFD applies to the STOT TPRS. This diagram illustrates IAFIS processing of an electronic Ten-Print Rapsheet Request initiated by an INS/ICE office using an IDENT Workstation. This search results in the return of the rapsheets for up to the top 20 candidates—an Ident/Non-Ident decision is *not* a part of this process. Additionally, images are not returned as part of this process.

(1) IAFIS receives the EBTS Ten-Print Fingerprint Search (E1020) message from a remote INS/ICE office via the JABS network and the CJIS WAN. ITN/FBI prepares the Remote Ten-Print Fingerprint Search (A1020) message. This message contains the FILEHANDLE that AFIS/FBI will use to retrieve the file containing the fingerprint submission images from ITN/FBI, formatted in accordance with I1020.

(2) AFIS/FBI will perform the requested search and send the Remote Ten-Print Search Candidate List (A1006) message to III/FBI.

(3) III/FBI performs filtering on the list of candidates. If any of the candidate records contain flags or codes indicating that the record requires special attention, III/FBI will send a Review Request (A1312) message to ITN/FBI that will be routed to a Special Stops Service Provider for review and processing.

(4) The result of the Special Stops Service Provider Review is returned in the Review Response (A1313) message sent from ITN/FBI to III/FBI.

(5) III/FBI will format the Ten-Print Rapsheet Request Response (A1025) message and send it to ITN/FBI which will forward it to EFCON which will return it to the remote INS/ICE office via the CJIS WAN and the JABS network as the Ten-Print Rapsheet Request Response (E1025) message.

Figure 22.3-01 External III/FBI File Maintenance Request (EHN) Data Flow Sequencing and Notes

This DFD applies to the STOT EHN. This data flow shows how a III participant EHN File Maintenance Request is processed by IAFIS. While the majority of supplemental identifiers in a subject criminal history record will be entered as the result of fingerprint submissions, a state may have documentation concerning aliases, additional dates of birth, etc., not provided to the FBI. This may occur when the state processes a fingerprint card for a non-serious offense. An EHN message is to be used by III participants to add one or more supplemental identifiers to a subject record. This message can also be used to seal a subject arrest record related to a particular state.

(1) IAFIS receives a III Supplemental Identifier Request-EHN (N3207) message via NCIC.

(2) III/FBI processes the request and returns the Supplemental Identifier Accept Response (N3208) message. The response may be either an acknowledgment that the request was successfully processed or a reject response. The message (N3208) is sent to the requester via NCIC.

(3) Only if the EHN request added descriptors to a subject record will III/FBI send the new subject descriptor set to ITN/FBI in the File Synchronization Request (A3045) message.

(4) ITN/FBI sends an Update Descriptive Data Request (A3312) message to AFIS/FBI.

(5) The following is a list of unsolicited reports that may be spawned from processing an EHN File Maintenance Request. These reports will be formatted by III/FBI and sent to ITN/FBI in the Unsolicited Report (A3150) message to be printed on desktop printers in ITN/FBI.

Report Title	Destination Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
III Participant Online Printer Response - Hit Against SPF 5, 6, C, K, N, or DOD	Special Stops Unit

The following is a list of messages which may be spawned from processing an EHN File Maintenance Request. The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification
N3121 Single State Offender Status Notification (SSO)
N3112 Multi-State Offender Status (MSO)

Figure 22.3-02 External III/FBI File Maintenance Request (XHN) Data Flow Sequencing and Notes

This DFD applies to the STOT XHN. This data flow shows how a III participant XHN File Maintenance Request is processed by IAFIS. An XHN transaction is used to cancel a specific supplemental identifier from a subject record. On-line cancellation of a supplemental identifier is allowed only for single-state records. The designated state agency transmitting the XHN transaction must be the state of record. On-line cancellation of a supplemental identifier in a multi-state record will not be allowed because the index is shared and the identifier may be applicable to another state or Federal record.

(1) IAFIS receives the III Cancel Supplemental Identifier Request-XHN (N3211) message via NCIC.

(2) III/FBI performs initial validation on the request. If the message fails this validation, III/FBI sends a Cancel Supplemental Identifier Accept Response—XHN (N3212) message containing the III Single-Line Reject Message report (see III Pspec Supervisor Appendix D) to the requestor via NCIC and terminates the transaction.

If the message passes validation III/FBI will process the message. If the requested record modifications are successful, III/FBI returns the N3212 containing the III XHN Accept Message report.

If the requested record modifications cannot be performed, III/FBI will send an N3212 message containing a Multiple-Line Reject report (refer to MDD, N3212 message conditions for details).

If III/FBI rejects the N3211 for any reason other than a failure of the initial validation, III/FBI will then send the Cancel Supplemental Identifier Accept Response—XHN (N3212)/III XHN Accept Response (N3212) messages containing the III XHN Accept Message report. **This will occur in addition to any previously initiated N3212 sent indicating transaction failure based on the data contained in the N3211.**

(3) If the XHN request deleted descriptors from a subject record, III/FBI will send the new subject descriptor set to ITN/FBI in the File Synchronization Request (A3045) message.

(4) If A3045 was received from III/FBI in (3), ITN/FBI sends an Update Descriptive Data Request (A3312) message to AFIS/FBI.

(5) The following is a list of unsolicited reports that may be spawned from processing an XHN File Maintenance Request. These reports will be formatted by III/FBI and sent to ITN/FBI in the Unsolicited Report (A3150) message to be printed on desktop printers in ITN/FBI.

Report Title	Destination Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
III Participant Online Printer Response - Hit Against SPF 5, 6, C, K, N, or DOD	Special Stops Unit

The following is a list of messages which may be spawned from processing an XHN File Maintenance Request. The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name
N3124 Unsolicited Activity Notification
N3121 Single State Offender Status Notification (SSO)
N3112 Multi-State Offender Status

Figure 22.3-03 External III/FBI File Maintenance Request (MRS) Data Flow Sequencing and Notes

This DFD applies to the STOT MRS. This data flow shows how a III participant MRS File Maintenance Request is processed by IAFIS. An MRS transaction is used by a III participant state to make changes to its SID or pointer in a subject record held in III/FBI.

Message Number/Name
N3112 Multi state Offender Notification
N3121 Single State Offender Status Notification
N3124 Unsolicited Activity Notification

(1) IAFIS receives a III Add, Modify SID Request –MRS (N3209) message via NCIC.

(2) III/FBI processes the request and returns an Add, Modify SID Response-MRS (N3210). The response may be an acknowledgment that the request was successfully processed or a reject response. The (N3210) message is sent to the requester via NCIC.

(3) The following is a list of unsolicited reports that may be spawned from processing an MRS File Maintenance Request. These reports will be formatted by III/FBI and sent to ITN/FBI in the Unsolicited Report (A3150) message to be printed on desktop printers in ITN/FBI.

Report Title	Destination Printer
III Unauthorized Access (UAA) Notification Message	Special Stops Unit
III Participant Online Printer Response—Hit Against SPF 5, 6, C, K, N, or DOD	Special Stops Unit

The following is a list of messages which may be spawned from processing an MRS File Maintenance Request. The messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Figure 22.3-04 Ad Hoc CCA Search and/or Update CCA Request Data Flow Sequencing and Notes

This DFD applies to the STOT CCAQ and CCAD. This diagram illustrates the messaging sequence used when a IAFIS or NICS Service Provider performs updates to records contained in the CCA File in III/FBI.

This flow represents the interaction of the ITN/FBI DPS Service Provider or NICS Service Provider as the record inquiry or update activity occurs. For an inquiry, the Service Provider will request the current record and receive the response.

(1) ITN/FBI or NICS sends the Ad Hoc CCA Search Request (A3010) message to III/FBI. This message is structured to accomplish either a direct record retrieval or an Ad Hoc search of the CCA file.

NOTE: The response message will be sent to whatever system (ITN/FBI or NICS) sent the request.

(2) If the A3010 contained ORI, III/FBI retrieves the requested record and returns it in the Ad Hoc CCA Direct Retrieval Response (A3011) message to ITN/FBI or NICS.

(3)If A3010 contained SIG, III/FBI will perform a search and return the matching CCA records in the Ad Hoc CCA Search Response (A3015). If the search finds more than 200 matching AD-HOC-CCA-DATA sets, A3015 will return the first 200.

This flow represents the interaction of the ITN/FBI DPS Service Provider as the file update activity occurs. The Service Provider initiates a request to update the record and receives an indication of the success or failure of the maintenance action.

(4) ITN/FBI initiates the CCA Update Request (A3043) message containing an update to a record in the CCA File.

(5) III/FBI performs the requested update and returns the File Maintenance Response (A3027) message to ITN/FBI to be displayed to the Service Provider.

Figure 22.3-05 File Comparison Data Flow Sequencing and Notes

This DFD applies to the STOT FCOM. This data flow shows the initiation of the File Comparison Function by the ITN/FBI Segment Administrator, the associated message flows among ITN/FBI, III/FBI and AFIS/FBI, and the generation of the final reports. The criminal bitmap comparison includes only those FNUs that are active in III/FBI with fingerprints in ITN/FBI.

The ITN/FBI Segment Administrator (ITN/FBI SA) initiates a file comparison request for either the criminal files (i.e., Criminal Ten-Print Fingerprint Image Master File, Criminal Ten-Print Fingerprint Features Master File, Subject Criminal History File) or the civil files (i.e., Civil Ten-Print Fingerprint Image Master File, Civil Ten-Print Fingerprint Features Master File, Civil Subject Index Master File) as defined by the NDR value in the A3012.

(1) The File Comparison Bitmap Request Message (A3012) is sent to III/FBI and AFIS/FBI to request the FNU Bitmap for the criminal files or the Civil Record Number (CRN) Bitmap for the civil files. This is determined by the ITN/FBI SA at the time (see (1) above).

(2) The File Comparison Bitmap Request Response Message (A3013) is sent from III/FBI and AFIS/FBI to return the FNU Bitmap for the criminal files or the CRN Bitmap for the civil files. The bitmaps contained in A3013 are compressed using a lossless compression algorithm.

Upon receipt of message A3013 from both III/FBI and AFIS/FBI, ITN/FBI will decompress the bitmaps, compare the bitmaps for the three segments and, if necessary, produce discrepancy and persistency reports.

Figure 22.3-06 NARA Records Archival and Purging Data Flow Sequencing and Notes

This functionality is not used, has not been used, had no SP/CRs written against it, and, while there is desire to use it, there has been no real action to make that happen.

This DFD applies to the STOT NAP. This data flow shows how automated criminal identification record information is transferred via magnetic tape to the National Archives and Records Administration (NARA). The retrieval criteria (i.e., year of Birth, Date of Death Notification) used for criminal history record archival is based on records disposition agreements established between the FBI and NARA.

(1) The III/FBI segment administrator sets the parameters for selection and medium of exchange.

(2) Purged criminal records due to death or exceeding age limit are transferred to tape. All related indices and Computerized Records Sent data are purged.

(3) The File Synchronization Request (A3045) message is sent to ITN/FBI to initiate file synchronization.

(4) ITN/FBI tells AFIS/FBI to delete fingerprint features and descriptive data of the archived or purged subjects. One Delete Fingerprint Features Request (A3321) message will be sent for each subject to be deleted.

Figure 22.3-07 NCIC and Nlets Administrative Messages Sequencing and Notes

This diagram illustrates IAFIS handling of administrative messages received from NCIC and Nlets.

(1) IAFIS will receive the NCIC Administrative Message (N3601). ORI and Line Number Validation are performed at the F/E. These messages are then routed to the System Administrator console.

Figure 22.3-08 CRS Update Request Data Flow Sequencing and Notes

This data flow applies to the STOT CRSD. This diagram illustrates the messaging sequence used when a Service Provider performs updates to the Computerized Records Sent (CRS) File in III/FBI.

This flow represents the interaction of the ITN/FBI DPS Service Provider as the record inquiry activity occurs. The Service Provider sends a request for the subject record and receives that record from the SCH file held in III/FBI.

(1) ITN/FBI sends the Criminal History Request (A1040) message (a request for RANR, refer to DFD 21.4-02) to III/FBI.

(2) III/FBI returns the Criminal History Request Response (A1042) message to ITN/FBI.

The ITN/FBI DPS Service Provider initiates a request to update the record and receives an indication of the success or failure of the maintenance action.

(3) ITN/FBI initiates the CRS Update Request (A3007) message containing an update to a subject record in the SCH File.

(4) III/FBI performs the requested update and returns the File Maintenance Response (A3027) message to ITN/FBI to be displayed to the Service Provider.

NOTE: Upon completion of the update, the Service Provider may initiate a second A1040/A1042 message pair to insure that the update was properly applied to the record.

Message Number/Name
N3124 Unsolicited Activity Notification

Figure 22.3-09 External III/FBI Disposition Maintenance Request (DSP) Data Flow Sequencing and Notes

This DFD applies to the STOT DSP. This diagram illustrated IAFIS processing of the External III/FBI Disposition Submission Request. This STOT provides expanded capabilities for the submission and retention of disposition information. III Participants will have the ability to submit disposition data via the National Crime Information Center (NCIC) to the III segment of the IAFIS utilizing a newly created disposition submission message.

(1) III/FBI receives the N3217 III DSP Request message via NCIC when a III Participant desires to add, append, replace or delete disposition data for an arrest that is already on file with the FBI.

(2) III/FBI validates the N3217 and should a successful automated update occur:

(a) if the updated record contains an SPF of 5, C, or N, an Unsolicited Report (A3150 containing a III Participant Online Hit Notification - Automated Document Update) is sent to the Special Stops Printer.

(b) if the updated record contains an SPF of I, L, or T, an Unsolicited Report (A3150 containing a III Participant Online Hit Notification - Automated Document Update) is sent to the Answer Hits to Wants Printer.

Or

(3) III/FBI validates the N3217 and if no successful automated update occurs, III/FBI determines if it is a conflict error:

(a) if the record to be updated contains an SPF of 5, C, or N, III/FBI sets the Document Log Destination (DLD) to 'S'.

(b) if the record to be updated contains an SPF of K or a DOD, III/FBI sets the DLD to 'D'.

(c) if the record to be updated contains an SPF of I, L, or T, III/FBI sets the DLD to 'W'.

(d) If none of the above SPF flags exist in the record to be updated, III/FBI sets the DLD to 'G'.

III/FBI formats the A3222 and sends it to ITN/FBI. ITN/FBI uses the DLD code from the A3222 and populates the appropriate Document Processing Log (DPL).

(4) The response may be either an acknowledgment that the request was successfully processed, was sent for conflict resolution, or a reject response. The N3218 III DSP Accept Response message is sent to the requester via NCIC.

The following unsolicited report may be spawned from processing a DSP Disposition Submission Request. This report will be formatted by III/FBI and sent to ITN/FBI in the Unsolicited Report (A3150) message to be printed on desktop printers in ITN/FBI.

Report Title	Destination Printer
Automated Update Notification	Special Stops or Answer Hits to Wants Units

The following is a list of messages which may be spawned from processing a DSP Disposition Submission Request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC telecom network.

Message Number/Name

N3124 Unsolicited Activity Notification

Figure 22.4-01 ORI File Update Data Flow Sequencing and Notes

This DFD applies to the STOT ORI. This diagram illustrates IAFIS handling of messages received from NCIC that are used to update the ORI Table.

(1) The $.A.ORI (N3020) message is received by IAFIS. III/FBI performs update(s) to the ORI File.

Figure 22.4-02 Line File Update Data Flow Sequencing and Notes

This DFD applies to the STOT LIN. This diagram illustrates IAFIS handling of messages received from NCIC that are used to update the Line File in III/FBI.

(1) The $.A.LIN (N3021) message is received by IAFIS. ORI and Line Number validation will be performed upon receipt of the message. III/FBI performs requested update(s) to the LIN File. Each line in the LIN File comprises an individual message. Should validation fail, an exception is generated within III/FBI and no update is performed.

OR

(2) The $.A.LIN (N3019) message is received by IAFIS. ORI and Line Number validation will be performed on message. The complete LIN Table is replaced. Should validation fail, an exception is generated within III/FBI, and no update is performed.

Figure 23.4-02 TI$ Test Request Data Flow Sequencing and Notes

This DFD applies to the STOT TIR. This data flow shows how an external TI$ Test Request is processed by IAFIS.

(1) The III/FBI TI$ test records are available to the III participating states for testing receipt of the $.A. unsolicited messages. The single-state and multi-state test records provided by each state will be used by III/FBI to construct the test messages. The message key for accessing the III/FBI test records is TI$. To receive $.A. messages, the state must send a TI$ Request (N5100) message to IAFIS to produce transmission of <u>one</u> or <u>all</u> the applicable $.A. messages.

(2) The response for a TI$ request is the $.A. message. III/FBI will respond with the TI$ Response (N5101) message. This Message is prepared and sent to the external user via the NCIC network. This flow will only exist, if a reject or a state system requires an "Accept" response to its request. When the TI$ message contains an error, a reject response will be contained in this response.

The following is a list of messages which may be spawned from processing a TI$ test request. These messages will originate from III/FBI for a destination outside IAFIS via the NCIC Network.

<u>Message Number/ Name</u>
N3102 (CFN) No Prior Record—Civil
N3103 (CFR) Prior Record—Civil
N3105 Unsolicited Criminal History Record Request
N3106 Consolidated Notification
N3107 Unsolicited Decease Notification
N3108 FNU Expungement Notification
N3109 SID Expungement Notification
N3112 Multi-state Offender Status Notification
N3114 Non-matching SID
N3115 No Prior Record—SID Entered
N3116 Prior Record—Previously Entered SID (Single)
N3117 Prior Record—SID Entered
N3118 Reactivate Expunged Cycle Notification
N3119 Reject No Prior Record—SID Not Entered
N3120 Reject Prior Record—SID Not Entered
N3121 (SSO) Single State Offender Status Notification
N3123 Prior Record—Previously Entered (SID) (Multi)

Figure 24.1-01 iDSM File Maintenance (IAFIS Data)

This DFD applies to the addition and deletion of IAFIS-supplied data to iDSM. This data flow illustrates iDSM processing of IAFIS-supplied data from the Wants and Warrants or Known or Suspected Terrorist tables. The Files used in the process include the Criminal Ten-Print Fingerprint Image Master File (FIMF) (ITN/FBI) the Subject Criminal History File (SCH) (III/FBI), and the iDSM Candidate Repository.

Each night, III performs a query to select candidates from the Want table and the Known or Suspected Terrorists table with AUD=Blank and AUD='N.' The results of this query are stored in a flat file and moved to iDSM using a secure copy data transfer.

When the flat file is received by iDSM/FBI, each FNU will be compared to the iDSM candidate repository. Based on the compare results the candidate will either be added, demoted or deleted. If the candidate FNU is not found, it will be added.

(1) Based on the FNU in the flat file, iDSM/FBI creates an FNU add/demote/delete request (WList_RQS_WS_VIPS/process) and transmits the message to iDSM/DHS.

(2) When iDSM/DHS receives the WList_RQS_WS_VIPS/process message, it will update the iDSM candidate record by either adding, demoting or deleting the candidate. If adding, iDSM/DHS creates a new record. If deleting, iDSM/DHS removes the candidate from its list. If demoting, iDSM/DHS determines if there is any activity on their record. If there has been activity on the record, iDSM/DHS demotes the record; if there has been no activity on the record, iDSM/DHS deletes the record. Upon completion of this task, iDSM/DHS returns a confirmation message to iDSM/FBI, WList_RSP_WS_CIMS/process.

Figure 24.1-02 iDSM File Maintenance (IDENT Data)

This DFD applies to the addition and deletion of IDENT-supplied data to iDSM. This data flow illustrates iDSM processing of IDENT-supplied data from the Biometric Visa Denial and Expedited Removals data sets. The Files used in the process include the iDSM Candidate Repository.

Every two weeks, IDENT selects candidates from the Biometric Visa Denial and Expedited Removals data sets.

(1) iDSM/DHS then sends all selected candidates to iDSM/FBI individually via the DHS_BIOMETRICS_Request message. Upon receipt of the individual candidate messages, iDSM/FBI adds or deletes the candidates as specified in the message.

(2) When iDSM/FBI receives the DHS_BIOMETRICS_Request, it will insert or delete the specified candidate data. iDSM/FBI will return the WLIST_RSP_WS_VIMS/send_confirmation message to iDSM/DHS.

Figure 24.1-03 iDSM Search of IAFIS Submissions

This DFD applies to the search of an IAFIS submission against iDSM/FBI. This data flow illustrates iDSM processing of IAFIS submissions which qualify for iDSM search. The File used in the process is the iDSM/FBI Candidate Repository.

When an IAFIS Ten-Print submission from a pilot agency meets the criteria for search against the iDSM database (see Figure 21.1-01a), EFCON/FBI will forward the submission details to iDSM/FBI as a post. Upon receipt of the post, iDSM/FBI will search its repository for matching candidates.

(1) When the search completes, iDSM/FBI retrieves the images, via the WBio_RQS_WS_VIMS/retrieve message (from ITN/FBI), of any candidate whose match score is high enough to qualify for Fingerprint Image Compare (see figure 21.1-01a for a complete description of the FIC process).

When the images have been retrieved, the submission is forwarded to a FIC service provider who will make an Identification or Non-Identification decision. This decision is sent to the contributor via e-mail.

Prior to sending an identification notification to the contributor, an IAQ Message is sent via Nlets to LESC to retrieve any additional biographic and immigration data in the form of an IRR. The IRR data is added as rapsheet data. This compiled response is then sent to the contributor.

APPENDIX C NCIC /NLETS INTERFACE COMMUNICATIONS REQUIREMENTS

The references to the implementation of control characters STX and ETX apply to the IAFIS interface to Nlets also.

C.1 Interface Description

C.1.1 i. The IAFIS will support one well-known listener socket (one IP address and one port) used to coordinate the receipt of NCIC-to-III messages. NCIC will support one well-known listener socket used to coordinate the receipt of III-to-NCIC messages. The relationship between the two III-NCIC interfaces will be asynchronous, in that response messages from III to NCIC may be in a different sequence from that in which the query was received and may include unsolicited messages. To initiate message transmission, the sender (either NCIC or III) will request a socket connection of the receiver (III or NCIC) using standard TCP/IP socket protocols. This allows the receiver to support concurrent connections.

ii. III/FBI will support one socket pair (sender socket and receiver socket) used to coordinate messaging between III and Nlets. The relationship between these sockets is also asynchronous, but each individual socket supports synchronous communications through the use of application level acknowledgements.

C.1.2 i. The sender (IAFIS or NCIC) will open the indicated socket for transmitting. The transmitted character stream will start with a four byte pattern (Hex 'FF00AABB'), followed by a 2 byte length, and then an NCIC header and request or response text followed by a four byte end pattern (Hex 'BBAA00FF'). Acknowledgements are handled by the TCP/IP protocol with no additional application-level acknowledgments. Request or response text will end with the archaic Bi-Sync character EOT (Hex '004') as the III application still requires this character to be present.

ii. Nlets messages are framed by the same starting and ending bytes, but use a four byte length and additional application headers as defined in the Nlets Operating Manual. Message segmentation is supported, and application-level acknowledgements are used in accordance with the Nlets Operating Manual

C.1.3 i. A Successful write to the NCIC socket is considered by the III application to be the end of a particular communication. No retry logic is built in to the application layer.

ii. The message retry logic on the III/Nlets interface is a function of the Nlets design and is not described herein.

C.1.4 If a message from III to NCIC is blocked, a successful write of the first block will lead to subsequent blocks being written to the socket.

C.1.5 i. Messages from NCIC to III will never exceed one block. III performs validation of the NCIC header before parsing and processing the message body. If the header contents are not valid, an application level reject is returned to NCIC.

ii. Messages received via the Nlets interface can be multi-blocked.

C.1.6 Messages from NCIC are communicated directly to III/FBI. This includes external requests, Want/Sex Offender updates, Line/ORI file updates, and NCIC Administrative messages.

i. Nlets messages will be forwarded directly to III/FBI. III/FBI will aggregate consecutively received blocks in a single message which is terminated by the text "END OF RECORD." The IAFIS header will be constructed in accordance with C.5.1.vii.

ii. III communications layer software will build an IAFIS header for each non-administrative incoming NCIC message. This header is used only locally within the III application. III application software requires the presence of the IAFIS header because it was initially designed to receive the NCIC messages as IAFIS inter-segment messages from the ITN segment.

C.1.7 In the event of a III/FBI outage (III/FBI is unable to accept NCIC messages), the messages may queue up in the TCP/IP "pipe" unless III is taken out of service by NCIC operators, at which point NCIC will queue the III messages.

C.2 Update NCIC ORI File Processing

C.2.1 III/FBI will convert all letters "O" (capital alphabetic "oh") in ORI character positions 3 through 9 to "zero."

C.2.2 III/FBI will update its NCIC ORI File as directed by the MKE in the $.A.ORI message. If the MKE is "XO," III/FBI will delete the NCIC ORI File entry identified by the converted ORI from this message. If the MKE is "EO," then III/FBI

will add an NCIC ORI File entry identified by the converted ORI from the $.A.ORI message and including the ORI Type (element ORITYP, referred to as UCD). If the MKE is "MO," then III/FBI will replace the relevant data in the NCIC ORI File entry identified by the converted ORI from the $.A.ORI message.

C.2.3 If the ORI being deleted (MKE="XO") or modified (MKE = "MO) does not exist in the NCIC ORI File, if the ORI being added (MKE-"EO") already exists, or if a III/FBI failure precluded updating the NCIC ORI File, then III/FBI will log a software exception.

C.3 Update Line Number Table Processing

C.3.1 NCIC will send the $.A.LIN message to III/FBI.

C.3.2 III/FBI will process the $.A.LIN according to the MKE included in the N3021 message. The N3019 message will replace the entire Line Number Table.

C.4 III Request Message Authorization Processing Requirements

C.4.1 III/FBI will ignore any trailing blanks in the MKE value during authorization processing.

C.4.2 If the MKE value does not correlate to MTC of III as defined in MDD MKE/MTC Code Table, then III/FBI will respond with SLR type 7 as described in the MDD.

C.4.3 III/FBI will edit a copy of the received ORI as follows:

i. If character 9 is a numeric value, then set characters 8 and 9 to zero.

ii. If character 9 is "R," then set character 8 to zero.

iii. If character 8 is "J," then set character 8 to "7."

iv. III/FBI will convert all letters "O" (alpha "oh") in ORI character positions 3 through 9 to zero.

C.4.4 III/FBI will then perform the authorization checks of Table P-2 using the edited ORI. The check specified in line #20 of Table P-2 will be made against the converted value of STE; that is, any alpha 'O' will be replaced with a zero (e.g., "OH" will be converted to "0H"). If the Table P-2 check indicates an unauthorized or invalid ORI, then III/FBI will record the access attempt in the security log in addition to producing the SLR 6, 7, or 8 messages.

C.4.5 None of the authorization processing performed by III/FBI requires use of the CCA File.

C.5 NCIC Intersegment Message Requirements

C.5.1 In constructing the intersegment message used for sending the NCIC message to the III application, the III communications layer software will do the following:

i. Assign values to the elements of the IAFISHDR of the intersegment message;

a. Copy the received ORI into the ORI field of the IAFISHDR, except that ORI and Line Update and Want Notification messages use the default ORI;

b. Assign the STOT value applicable to the received MTC/MKE;

c. Copy the NCIC message as received, from the character following the length bytes and through the ending EOT character, into the data portion of the intersegment message.

ii. The III application layer will perform all other NCIC message validation as appropriate and then respond with an NCIC reject message, the related NCIC request response, or no response, as appropriate.

iii. III will log a software exception for errors in the IAFISHDR or empty NCIC data field or invalid NCIC data length, or failure of the III/FBI segment process handling NCIC messages.

C.5.2 All messages sent to NCIC will be completely formatted and blocked by III/FBI. An NCIC message (including all blocks) will be encapsulated as a contiguous data stream along with a count of the characters in the data stream.

C.5.3 In formatting NCIC responses and unsolicited messages, III/FBI will use the protocol defined in C.1.2.

C.6 Nlets Intersegment Message Requirements

C.6.1 Nlets messages are received by the III communications layer, an IAFIS header is built and the received message is incorporated into an IAFIS inter-segment message. This message is then passed into the III application. The IAFIS header is required by the III application, which was originally built around the concept of ITN/FBI receiving the Nlets message and forwarding to III. III application software will manage the association of the Nlets messages with the appropriate request and determine when all data blocks associated with one response have been received.

APPENDIX D RESPONSE GENERATION CSCI REPORTS FORMATS

INTRODUCTION

Response Generation CSCI Reports Formats are now found in the III Software Design Document, Response Generation Appendix D, located on the Omninet UNIX server steelhead.

APPENDIX E FBI NUMBERS & CHECK DIGITS

E.1 Introduction

FBI numbers are assigned to individuals as they are initially added to the FBI's Criminal files. An FBI number is comprised of up to three parts: one to seven numeric characters, an alphabetic suffix, and a numeric check digit. Over the years, four different formats have been used, and all four currently reside in the existing IAFIS. These formats are defined below.

Format 1. One to seven numeric characters with no suffix or check digit, e.g., 3134564. When the FBI number consists of seven numerics, the first numeric cannot be a seven or an eight. That is, there are no FBI numbers in the seven million or eight million range. Those seven numeric FBI numbers beginning with a nine (i.e., in the nine million range) represent IAFIS test records. This is the earliest format for an FBI number.

Format 2. A later format consists of one to six numeric characters plus a single alphabetic character as a suffix and no check digit, e.g., 789C. The valid alphabetic suffix characters are A through H.

Format 3. The next variation consists of one to six numeric characters, a single alphabetic character as a suffix, and a one to two-character numeric check digit, e.g., 2468J6.

For this format, the valid alphabetic characters for the suffix are

J	K	L	M	N	P	R
S	T	V	W	X	Y	Z

However, FBI numbers one (1) through 99,999 for S and Y suffixes are invalid.

The check digit will have a range from one (1) through eleven (11).

Format 4. The current format for an FBI number consists of one to six numeric characters, a two-character alphabetic suffix and one numeric check digit, e.g., 222144KA0.

For this format, the valid alphabetic characters for the first position of the suffix are

A	C	D	E	F	H	J
K	L	M	N	P	R	T
V	W	X				

The invalid characters for the first position are

B G I O Q S U Y Z

The only alphabetic characters currently allowed for the second character are A, B, and C[3]. In this format, the second alphabetic character is referred to as the "series" character and is not considered when computing the check digit.

The check digit will have a range from zero (0) through nine (9)

E.2 FBI Number Check Digit Calculation

1. For Formats 3 and 4, the first or only alphabetic suffix character is assigned a numeric value as shown in the Table E-1, below.

Table E-1 Suffix Value Assignments

Suffix	Value
A and J	1
K and S*	2
C, L, and T	3
D and M	4
E, N, and V	5
F and W	6
P and X	7
H and Y*	8
R and Z	9

The characters with the asterisk (*) in Table E-1 are valid for the single suffix of Format 3 but not valid as the first suffix in Format 4.

[3]As of May 30, 1997, the current two-character suffix in use is EB. Also note that SC is a valid two-character suffix but is never assigned to an FBI number. Depending on the life span of IAFIS the second allowable character in a two-character suffix may be expanded to include D, E, F, etc.

2. Each numeric character retains its value.

3. Each numeric character and the first or only alphabetic suffix are assigned to a position multiplier or weight as indicated below. The second alphabetic character in a two-character suffix, the series character is not assigned a multiplier[4].

FBI number:	N	N	N	N	N	N	A	a
Position Multiplier:	2	7	6	5	4	3	2	

Six numeric characters are needed to compute the check digit. Leading zero(s) must be used when the numeric portion is less than six characters.

4. Multiply the numeric value of each character (N) and the value assigned to the suffix (A) in the FBI number by its assigned position multiplier, and add the products to get the sum.

5. Divide the sum by eleven (11), then subtract the remainder from eleven (11). The difference will be the check digit, if not modified by the following rules:

a) When the sum is evenly divided by eleven (11), and the FBI number has a single alphabetic suffix, the check digit is set to eleven (11).

b) If the computed check digit is equal to eleven (11) and the FBI number has a two-character alphabetic suffix, the FBI number is NOT valid.

c) If the computed check digit is equal to ten (10) and the FBI number has a two-character alphabetic suffix, the check digit is set to zero (0).

Example 1: Single Alphabetic Character Suffix

FBI number: 2468J

A. Add leading zeros (0): 002468J

B.

FBI Number		Position Multiplier		Products
0	x	2	=	0

[4]The following notation is used in this section: 'N' will represent a numeric character, 'A' will represent the first or only suffix, and 'a' will represent the series character.

	0	x	7		=	0
	2	x	6		=	12
	4	x	5		=	20
	6	x	4		=	24
	8	x	3		=	24
J =	1	x	2		=	2
				Sum	=	82

C. Divide the sum by eleven (11): 82/11 = 7 with a remainder of 5.

D. Subtract the remainder from eleven (11): 11–5 = 6. Therefore, the full FBI number is: 2468J6.

Example 2: Two Characters Alphabetic Suffix

FBI number: 222144KA

A. No leading zeros (0) are necessary.

B.

FBI Number		Position Multiplier		Products
2	x	2	=	4
2	x	7	=	14
2	x	6	=	12
1	x	5	=	5
4	x	4	=	16
4	x	3	=	12
K= 2	x	2	=	4
		Sum	=	67

C. Divide the sum by eleven (11): 67/11 = 6 with a remainder of 1.

D. Subtract the remainder from eleven (11): 11–1 = 10. The check digit is set to zero (0) because the suffix has two alphabetic characters. Therefore, the full FBI number is 222144KA0.

APPENDIX F USING BITMAPS FOR FILE COMPARISONS

F.1 Introduction

Sequentially increasing number series are used to establish FBI numbers (FNUs) and Civil Record Numbers (CRNs). For FNUs, each series starts from one and increases sequentially up to a maximum of 999,999 within a given suffix identifier. A suffix identifier is typically a one- or two-letter combination which can be used for one or more years. For example, in 1967 through 1968, FNUs were established using numbers 1G through 999,999G. From September 4, 1990 through June 25, 1991 FNUs were assigned using numbers 1MA through 999,999MA[5]. CRNs are in only one series. This series starts with V00000001 and increases sequentially up to a maximum of V99999999.

The bitmap process identifies criminal and civil database synchronization errors by comparing bitmapped lists of the record identifiers (FNU or CRN) currently active in each segment and then reporting the differences.

F.2 Using a Bitmap

A bitmap scheme can record whether a given FNU is being used[6]. The scheme is to use a 1 bit flag for each possible identifier in the series. The bit will be set (=1) if the identifier is active, and reset (=0) if the identifier is not active. Figure F-1 illustrates the scheme for a sample of eight FNUs. Reading the figure from right to left, it shows that FNUs one through four and six through eight are being used, whereas FNU five is not.

Bitmap:	1	1	1	0	1	1	1	1
FNU:	8	7	6	5	4	3	2	1

Figure F-1 Scheme for FNU In-use Status

Because the identifier assignment algorithm is sequentially increasing, the position of the bit in the sequence indicates the exact identifier. Hence, a bitmap containing 999,999 bits could record the status of every FNU within a particular suffix (125,000 bytes or 31,500 32--bit words). A civil bitmap containing 99,999,999 bits (12,500,000 bytes or 3,125,000 32-bit words) could record the status of every CRN.

---

[5]Refer to the *Criminal Justice Information Services Division Automated Fingerprint Processing Operations Quality Control (QC) Guide*, dated November 1, 1993.

[6]This appendix illustrates the use of bitmaps for comparing FNUs across the three IAFIS segments. In fact, bitmaps can be used to compare any sequentially increasing series of numbers, such as Civil Record Numbers (CRNs).

These bitmaps will have to be maintained dynamically, or generated upon demand, to indicate the current status of an identifier. That is, for example, every time an FNU is added to (e.g., new subject) or deleted from (e.g., expunged) the Fingerprint Image Master File, the corresponding bit for that FNU series will be set or reset. An initialization process in each segment will be needed to create the initial bitmaps by setting the corresponding bit for each active FNU.

To accomplish a three-segment file comparison of identifiers, each segment will have to maintain its own bitmaps. The comparisons will be accomplished by having III/FBI and AFIS/FBI send copies of their bitmaps to ITN/FBI. ITN/FBI, in turn, will perform bitmap position comparisons to identify occurrences where the three bits are not the same.

F.3 Number of Bitmaps

It will require up to 74 bitmaps to handle the four possible formats of the FNU. These formats are defined in detail in Appendix E. A summary is provided in table F-1.

Table F-1 Number of Bitmaps per FNU Format

Format	FNU Format Description	Maximum FNUs per Format	Number of Bitmaps per Format
1	Seven numeric characters No primary Suffix No Secondary Suffix No check digit	9,999,999	1
2	Six numeric characters Primary Suffix: A—H No Secondary Suffix No check digit	999,999	8
3	Six numeric characters Primary Suffix: J-N, P, R-T, V-Z No Secondary Suffix Check digit (1-11)	999,999	14
4	Six numeric characters Primary Suffix: A, C-F, H, J-N, P, R, T, V-X Secondary Suffix: A, B, C Check digit (0-9)	999,999	51

F.4 Organization of Bitmaps

Figure F-1 shows eight FNUs stored right to left using eight bits, with FNU one occupying the right-most bit and FNU eight occupying the left-most bit. Because these eight bits represent 1 byte of storage, the FNUs are stored, in order, starting from the least significant bit (LSB) to the most significant bit (MSB). IAFIS will be using this scheme of 4 byte words as the storage unit size. It is imperative that this scheme is followed to avoid differences in word sizes across hardware platforms and computer languages. For example, consider the following:

```
        MSB          LSB    MSB          LSB    MSB          LSB    MSB          LSB
         1 1 1 1 1 1 1 1      1 1 0 1 1 1 0 1      1 1 1 1 0 1 1 1      0 1 1 1 1 1 1 1
             Byte 4               Byte 3               Byte 2               Byte 1
        MSB                                                                    LSB
        ---------------------------------4 byte word-------------------------------
FNU/CRN 32 ^ ^ ^ ^ ^ ^25   24 ^ ^ ^ ^ ^ ^17    16 ^ ^ ^ ^ ^ ^ 9    8 7 6 5 4 3 2 1
```

In this example, FNUs or CRNs 8, 12, 18, and 22 in the series are not in-use. This scheme continues with the next 4-byte word. Identifier 64 would be represented by the MSB and identifier 33 by the LSB in word 2. The number of identifiers in each series is increased by one to make the number of words per series an even multiple of 4 bytes. This last identifier is just a place holder and is never used.

The bitmaps for the four FNU formats will be organized in one file which contains 2,593,750 4-byte words. The organization of this file is shown in Table F-2, below. The organization treats the 74 bitmaps as one long bit stream. For example, FNU 1 for the CA suffix would be accessed by retrieving the least significant bit of word 1,031,251. Also FNU 999,999 for the CA suffix would be accessed by retrieving the bit immediately to the right of the most significant bit in word 1,062,500 (FNU 1,000,000 is never used, as mentioned above).

Table F-2 Organization of FNU Bitmap File

FNU Format	Primary Suffix	Secondary Suffix	Check Digits	First 4-byte Word	Last 4-byte Word
1	none	none	none	1	312,500
2	A		0	312,501	343,750
2	B		0	343,751	375,000
2	C		0	375,001	406,250
2	D		0	406,251	437,500
2	E		0	437,501	468,750
2	F		0	468,751	500,000
2	G		0	500,001	531,250
2	H		0	531,251	562;500
3	J		1 or 2	562,501	593,750

FNU Format	Primary Suffix	Secondary Suffix	Check Digits	First 4-byte Word	Last 4-byte Word
3	K		1 or 2	593,751	625,000
3	L		1 or 2	625,001	656,250
3	M		1 or 2	656,251	687,500
3	N		1 or 2	687,501	718,750
3	P		1 or 2	718,751	750,000
3	R		1 or 2	750,001	781,250
3	S		1 or 2	781,251	812,500
3	T		1 or 2	812,501	843,750
3	V		1 or 2	843,751	875,000
3	W		1 or 2	875,001	906,250
3	X		1 or 2	906,251	937,500
3	Y		1 or 2	937,501	968,750
3	Z		1 or 2	968,751	1,000,000
4	A	A	1	1,000,001	1,031,250
4	C	A	1	1,031,251	1,062,500
4	D	A	1	1,062,501	1,093,750
4	E	A	1	1,093,751	1,125,000
4	F	A	1	1,125,001	1,156,250
4	H	A	1	1,156,251	1,187,500
4	J	A	1	1,187,501	1,218,750
4	K	A	1	1,218,751	1,250,000
4	L	A	1	1,250,001	1,281,250
4	M	A	1	1,281,251	1,312,500
4	N	A	1	1,312,501	1,343,750
4	P	A	1	1,343,751	1,375,000
4	R	A	1	1,375,001	1,406,250
4	T	A	1	1,406,251	1,437,500
4	V	A	1	1,437,501	1,468,750
4	W	A	1	1,468,751	1,500,000

FNU Format	Primary Suffix	Secondary Suffix	Check Digits	First 4-byte Word	Last 4-byte Word
4	X	A	1	1,500,001	1,531,250
4	A	B	1	1,531,251	1,562,500
4	C	B	1	1,562,501	1,593,750
4	D	B	1	1,593,751	1,625,000
4	E	B	1	1,625,001	1,656,250
4	F	B	1	1,656,251	1,687,500
4	H	B	1	1,687,501	1,718,750
4	J	B	1	1,718,751	1,750,000
4	K	B	1	1,750,001	1,781,250
4	L	B	1	1,781,251	1,812,500
4	M	B	1	1,812,501	1,843,750
4	W	B	1	2,000,001	2,031,250
4	X	B	1	2,031,251	2,062,500
4	A	C	1	2,062,501	2,093,750
4	C	C	1	2,093,751	2,125,000
4	D	C	1	2,125,001	2,156,250
4	E	C	1	2,156,251	2,187,500
4	F	C	1	2,187,501	2,218,750
4	H	C	1	2,218,751	2,250,000
4	J	C	1	2,250,001	2,281,250
4	K	C	1	2,281,251	2,312,500
4	L	C	1	2,312,501	2,343,750
4	M	C	1	2,343,751	2,375,000
4	N	C	1	2,375,001	2,406,250
4	P	C	1	2,406,251	2,437,500
4	R	C	1	2,437,501	2,468,750
4	T	C	1	2,468,751	2,500,000
4	V	C	1	2,500,001	2,531,250
4	W	C	1	2,531,251	2,562,500

FNU Format	Primary Suffix	Secondary Suffix	Check Digits	First 4-byte Word	Last 4-byte Word
4	X	C	1	2,562,501	2,593,750

Depending on the life span of IAFIS, the second character of a two-character suffix may have to be expanded to include D, E, F, etc. Consequently, FNU Bitmap File would be expanded by 531,250 words for each second character added. III/FBI also includes the bits reserved for the FNUs in series AD, CD, and DD in their criminal bitmaps to allow for their specified maximum criminal file sizes. These extra bits are ignored by ITN/FBI during the comparison process.

The bitmap for the CRN format will be organized as one series in one file containing 3,125,000 4-byte words. Because only one series exists, the bit representing each CRN can be determined through the following algorithm:

Word Number = ((CRN numeric–1) integer division by 32) + 1

Bit position in word (referencing MSB as 32 and LSB as 1 as shown in section F.4) =

[(CRN numeric–1) modulo 32] + 1

APPENDIX G IAFIS MESSAGE VALIDATION MATERIALS

G.1 Introduction

Appendix G contains information required for the message validation that is to be performed by IAFIS. This information includes:

- Description of the Originating Agency Identifier
- Rejection rules for III messages forwarded from NCIC to IAFIS
- Acceptance rules for EBTS messages received over the CJIS WAN by IAFIS

G.2 Originating Agency Identifier

The Originating Agency Identifier (ORI) is a unique nine character code assigned to each of 85,000 agencies that will be authorized to query the criminal files and/or provide criminal data to both the FBI NCIC and IAFIS systems. Section 13 of the *NCIC Operating Manual* defines the criteria for accessing these systems. The ORI will also be used to identify the additional agencies that will be using only the CJIS WAN to communicate with IAFIS. The first two characters of the ORI must be alphabetic and designate the state, territory, province, or country of the contributor or requester. The next three positions identify the county (3 numeric) in which the agency is located or a three-character acronym for federal agencies. Positions six through nine are used to identify the various types of entities within the type of agency. The format of the ORI based upon the type of agency is shown in Table G-1.

G.3 Rejection Rules for III Request Messages ($.A.III) Received from NCIC

IAFIS will receive III messages from the NCIC. Table G-2 provides rejection rules for$.A.III messages and assigns the rule validation to III/FBI (refer to Appendix C for specific NCIC message validation and processing requirements). III Request messages that satisfy any of the rules in Table G-2 are invalid. A validation based on ORI, NCIC Line, and Purpose Code is performed by III/FBI.

G.4. EBTS Message Validation

EBTS Message Validation is performed by EFCON/FBI. The EBTS Type-1 record ORI value must match that in a record in the EBTS ORI table maintained in EFCON/FBI. Upon finding a match, EFCON/FBI confirms that the TOT in the message is appropriate for any CWU autho-

rized for that ORI. Table G-3 provides a matrix relating CJIS WAN User codes (CWU) to EBTS TOTs. Shaded areas represent valid CWU and EBTS TOT combinations; white areas represent invalid CWU and EBTS TOT combinations. Test mode EBTS transactions ("T" suffix appended to the TOT) are validated in the same manner as operational mode EBTS transactions. When EFCON/FBI sends a response, it is returned to the e-mail address associated with the ORI in the EBTS ORI table.

Table G-1 Format of ORI Number Codes

Type of Agency	Positions 1-2	Positions 3-5	Positions 6-7	Positions 8-9
Law Enforcement ORIs	State, US, DC, PR, VI, province, or country	Three-character acronym for federal agency ORI or County (3 numerics) in which the non-federal agency is located for other ORIs	Used to distinguish one agency from another in the same county and/or indicate number of agencies within a county.	Zeros in positions 8 and 9 for a law enforcement ORI. NCIC users may use positions 8 and 9 to identify internal divisions, units, substations, or multiple terminals within the same agency/city except that position 9 cannot be an alphabetic character[7]
Criminal Justice ORIs	State, US, DC, PR, VI, province, or country	Three-character acronym for federal agency ORI or County (3 numeric) in which the non-federal agency is located for other ORIs	2 numbers uniquely distinguishing one agency from other agencies of the same type and level within the same county	position 8 indicates government level[8] (1=local, municipal, city; 3=county; 5=state; 7=federal; 9=nongovernmental). Position 9 contains A, B, C, E, F,G, J, M, N, Q, R, or Y (see note at end)
Agencies that do not meet NCIC criteria but are authorized to receive criminal history data and submit fingerprint cards to FBI	State, US, DC, PR, VI, province, or country	Three-character acronym for federal agency ORI or County (3 numeric) in which the non-federal agency is located for other ORIs	2 numbers uniquely distinguishing one agency from other agencies of the same type and level within the same county	Z in position 9
Agencies that are authorized to access NCIC files only	State, US, DC, PR, VI, province, or country	Three-character acronym for federal agency ORI or County (3 numeric) in which the non-federal agency is located for other ORIs	2 numbers uniquely distinguishing one agency from other agencies of the same type and level within the same county	K, P, V, or W in position 9 (see note at end)

Note for Position 9: A = Prosecuting Attorney's Office; B = Pretrial service agencies; C = Correctional Institutions; E = Nongovernmental railroad or campus police departments; F = Governmental social services agenciew that have been tasked with child protection responsibilities. To be used only in investigating, or responding to, reports of child abuse, neglect, or exploitation; G = Probation and Parole Offices; J = Courts, Magistrates Offices; K = Medical Examiners

---

[7] Positions 8 and 9 are also being used to assist State CSAs to identify and forward EBTS traffic to local agencies that use the State CSAs as intermediary communications centers.

[8] An exception is Code J for position 8 which indicates that agency does not meet all of the authorization requirements for the criminal justice category. Temporarily changing the code to a 7 makes it consistent for subsequent ORI File search editing.

and Coroners' Offices; M = Custodial Facilities in a medical or psychiatric institution and some medical examiners' offices; N = Regional dispatch center which is in a criminal justice agency, etc; P = Private campus police, railroad police, and "911" centers; Q = Authorized Public Housing authorities; R = Agencies authorized by Public Law 99-169 for national security purposes; V = Department of Motor Vehicles; W = National Center for Missing and Exploited Children; Y = Local, County, State, or Federal Agency which is classified as a criminal justice agency by statute, but does not fall into one of the above categories.

Table G-2 IAFIS FE NCIC III Request ($.A.III) 2000 Message Rejection Matrix

Chk No.	Segment Responsible for Check	EVALUATION CRITERIA						
		ORI Code Positions (Message ORI)	Message Key (Message MKE)	Line Address (Message LINE_ ADDRESS)	User Code (Line Table (UCD)	State Edit (Line Table STE)	ORI Type (ORI Table ORITYP)	Single Line Reject Type
1	Reserved							
2	Reserved							
3	Reserved							
4	III/FBI		not contained in MKE/MTC Code Table					7
5	III/FBI	9 = (K, P, U, V, or W)						8
6	III/FBI	1-7 = TXAF012						8
7	III/FBI	3-6=NICB						8
8	III/FBI	3-5 = USN	not (QH, QR, or QWI					8
9	III/FBI	1-4 = USMC OR: ********** 3-5 = MC0	not (QH, QR, QWI, or ZR) ********* not (QH, QR, QWI, or ZR)					8 ***** 8
10	III/FBI	3-5 = FBI	not (QH, QR, or QWI)	D71				8
11	III/FBI	3-5 = LEG	not (QH, QR, or QWI)					8
12	III/FBI	9=(A,B,C,G,J,) and 8≠(1,3,5 or 7)						6
13	III/FBI	1-9=NH008015H	not (QH, QR, or QWI)					8
14	III/FBI	ORI not in ORI File						6
15	III/FBI			LINE_ADDRESS not in Line Table				8
16	III/FBI	3-5 =FBI			not (04, 08, 36, 46, 51, 71, 89 or 90	XX		6

Chk No.	Segment Respon-sible for Check	EVALUATION CRITERIA						
		ORI Code Positions (Message ORI)	Message Key (Message MKE)	Line Address (Message LINE_ ADDRESS)	User Code (Line Table (UCD)	State Edit (Line Table STE)	ORI Type (ORI Table ORITYP)	Single Line Reject Type
17	III/FBI						E, F, R, S, Y, Z	8
18	III/FBI	1-2 ≠ (AB, BC,CD,IC, MB, NK, NF, NT, NS, 0N, PE, PQ, SN, or YT)				WW		6
19	III/FBI	1-2 ≠ (VI or PR)				ZZ		6
20	III/FBI	1-2 ≠ Converted (alpha 'O' to zero) STE value in Line Table				not (XX, WW, or ZZ)		8

Table G-3 CJIS WAN Transaction Authorization Matrix[9]

TOT	CWU	J Criminal Justice	F Civil-Federal	S Civil-State/ Local	L Latent Services	R Remote Services	M Multi-function User[10]	C Card Scanning Service Facility	I INS/ICE Remote
CAR									
CNA									
CPDR									
CPNU									
DEK									
DEU									
MPR									
AMN									
TPFS									
TPIS									
LFS									
CFS									
MCS									
ELR									

[9]Shaded cells indicate authorization for that TOT/CWU combination's CSA.

[10]A multi-function User is defined as a CSA authorized for all Criminal, State/Local Civil, Latent Services, and Remote Services TOTs.

TOT	CWU	J Criminal Justice	F Civil-Federal	S Civil-State/Local	L Latent Services	R Remote Services	M Multi-function User10	C Card Scanning Service Facility	I INS/ICE Remote
LFIS									
LFFS									
ULD									
ULAC									
IRQ									
FIS									
CPR									
CPD									
PHO									
FANC									
FAUF									
FNDR									
MAP									
NFAP									
NFUF									
NNDR									
LPNQ									
LSMQ									
LRSQ									
CARC									
CNAC									
DEKC									
FNCC									
FUFC									
MAPC									
NFFC									
SLCC									
FIDO									
NFDP									
TPRS									
NFUE									

TOT	CWU	J Criminal Justice	F Civil-Federal	S Civil-State/Local	L Latent Services	R Remote Services	M Multi-function User10	C Card Scanning Service Facility	I INS/ICE Remote
DOCE									

APPENDIX H INVALID STOTS FOUND ON THE OPERATIONAL ENVIRONMENT

Appendix H contains information found on the Operational Environment during a comparison of the STOTs to the documentation. These STOTs are invalid and will be removed. However, until a complete analysis can be done on the code, this appendix will serve as a reference guide.

STOT	Description	Segment
ARCHA	Undetermined.	ITN
INVLD	Possibly an invalid STOT was used.	ITN
MWCP	Undetermined.	ITN
NULL	Possibly used when no STOT is used.	ITN
SLCM	Special Latent Cognizant File Modify	ITN

APPENDIX I - iDSM PROTOTYPE

I.1 FBI iDSM Interface Technical Design

Each system within the DHS iDSM (VIPS and VIMS) will host its own set of web services with associated WSDLs. Each WSDL (or Web Service) will have an associated XML Schema Definition (XSD). The WSDL associates itself to a particular XSD by referencing the XSD within its Input and Output bindings. The Input binding corresponds to what input went into the web service. The Output binding corresponds to the output produced out of the web service.

I.1.1 SOAP Web Services Hosted on the DHS iDSM (VIPS)

WList_RQS_WS_VIPS
- Called by CIMS to pass WaW Biometrics information to VIPS and eventually IDENT.
- VIMS will pass back Acknowledgement Response to CIMS and eventually IAFIS.
- WSDL used
  - WList_RQS_WS_VIPS.wsdl
- XSD used
- FBI_Watch_RQS_VIPS.xsd (WaW Biometrics)

WHit_RQS_WS_VIPS
- Called by CIMS to pass ER Hit Notification or BVD Hit Notification to VIPS and eventually IDENT.
- CIMS will pass Acknowledgement Response to CIMS and eventually IAFIS.
- WSDL used
  - WHit_RQS_WS_VIPS.wsdl
- XSD used
  - FBI_Hit_RQS_VIPS.xsd (ER Hit Notification or BVD Hit Notification)

I.1.2 SOAP Web Services Hosted on the FBI iDSM (CIPS)

WList_RQS_WS_FF
- Called by VIMS to pass RC/A Biometrics or BVD Biometrics information to CIPS and eventually IAFIS.
- Acknowledgement Response will be passed back to VIMS and eventually IDENT.
- WSDL used
  - WList_RQS_WS_FF.wsdl
- XSD used
  - DHS_Watch_RQS_FF.xsd (RC/A Biometrics or BVD Biometrics)

WHit_RQS_WS_FF
- Called by VIMS to pass W/W Hit Notification to CIPS and eventually IAFIS.

- Acknowledgement Response will be passed back to VIMS and eventually IDENT.
- WSDL used
  - WHit_RQS_WS_FF.wsdl
- XSD used
  - DHS_Hit_RQS_FF.xsd (W/W Hit Notification)

I.1.3 SOAP Web Services Hosted on the DHS iDSM (VIMS)

WList_RSP_WS_VIMS
- Called by CIPS to pass ER/BVD Confirmation to VIMS and eventually IDENT.
- VIMS will pass Acknowledgement Response back to CIPS.
- WSDL used
  - WList_RSP_WS_VIMS.wsdl
- XSD used
  - DHS_Watch_RSP_VIMS.xsd (ER/BVD Confirmation)

WBio_RQS_WS_VIMS
- Called by CIPS to pass an FBI Image Request to VIMS.
- VIMS will pass Acknowledgement Response back to CIPS with or without image.
- WSDL used
  - WBio_RQS_WS_VIMS.wsdl
- XSD Used

FBI_Image_RQS_VIMS.xsd (FBI Image Request to DHS)

I.1.4 SOAP Web Services Hosted on the FBI iDSM (CIMS)

WList_RSP_WS_FD
- Called by VIPS to pass W/W Confirmation to VIMS and eventually IAFIS.
- Acknowledgement Response will be passed back to VIPS.
- WSDL used
  - WList_RSP_WS_FD.wsdl
- XSD used
  - FBI_Watch_RSP_FD.xsd (W/W Confirmation)

WBio_RQS_WS_DF
- Called by VIPS to pass DHS Image Request to VIMS.
- Acknowledgement Response will be passed back to VIPS and eventually IAFIS.
- WSDL used
  - WBio_RQS_WS_FD.wsdl
- XSD Used
  - DHS_Image_RQS_FD.xsd (DHS Image Request to FBI)

I.2 FBI iDSM XSD Formats

I.2.1 FBI_Watch_RQS_VIPS XSD

This represents a Want and Warrant Biometrics Web Service Request as well as its corresponding Web Service Acknowledgement Response.
FBI iDSM will send the message to DHS iDSM (CIMS to VIPS).
EBTS records coming from the FBI will include Subject Name, Image, Date of Birth, and Gender.
The FBI_Biometrics_Request element will map to the Input portion of the WList_RQS_WS_VIPS Web Service.
- Inputs into the web service call will conform to the fields listed within the FBI_Biometrics_Request element of the XSD.

The FBI_Biometrics_Response element will map to the Output portion of the WList_RQS_WS_VIPS Web Service.
- Outputs that result from the web service call will produce data that conforms to the fields listed within the FBI_Biometrics_Response element of the XSD.

I.2.2 FBI_Watch_RSP_CIMS XSD

Represents a Want and Warrant Biometrics Confirmation Response Web Service Request as well as its corresponding Web Service Acknowledgement Response
DHS iDSM will send the message to FBI iDSM (VIPS to CIMS).
The FBI_Confirmation_Response element is not functionally relevant.
The FBI_Confirmation_Request element will map to the Input portion of the WList_RSP_WS_CIMS Web Service.
- Inputs into the web service call will conform to the fields listed within the FBI_Confirmation_Request element of the XSD.

The FBI_Confirmation_Response element will map to the Output portion of the WList_RSP_WS_CIMS Web Service.
- Outputs that result from the web service call will produce data that conforms to the fields listed within the FBI_Confirmation_Response element of the XSD.

I.2.3 DHS_Watch_RQS_CIPS XSD

Represents an Expedited Removal or Biometric Visa Denial Biometrics Web Service Request as well as its corresponding Web Service Acknowledgement Response
DHS iDSM will send the message to FBI iDSM (VIMS to CIPS).
EBTS records coming from the US-VISIT will include Subject Name, Image, Date of Birth, and Gender
The DHS_Biometrics_Request element will map to the Input portion of the WList_RQS_WS_CIPS Web Service.
- Inputs into the web service call will conform to the fields listed within the

DHS_Biometrics_Request element of the XSD.

The DHS_Biometrics_Response element will map to the Output portion of the WList_RQS_WS_CIPS Web Service.

- Outputs that result from the web service call will produce data that conforms to the fields listed within the DHS_Biometrics_Response element of the XSD.

I.2.4 DHS_Watch_RSP_VIMS XSD

Represents an Expedited Removal or Biometric Visa Denial Biometrics Confirmation Response Web Service Request as well as its corresponding Web Service Acknowledgement Response

FBI iDSM will send the message to DHS iDSM (CIPS to VIMS).

The DHS_Confirmation_Response element is not functionally relevant.

The DHS_Confirmation_Request element will map to the Input portion of the WList_RSP_WS_VIMS Web Service.

- Inputs into the web service call will conform to the fields listed within the DHS_Confirmation_Request element of the XSD.

The DHS_Confirmation_Response element will map to the Output portion of the WList_RSP_WS_VIMS Web Service.

- Outputs that result from the web service call will produce data that conforms to the fields listed within the DHS_Confirmation_Response element of the XSD.

I.2.5 FBI_Hit_RQS_VIPS XSD

This represents an Expedited Removal or Biometric Visa Denial Hit Notification Web Service Request as well as its corresponding Web Service Acknowledgement Response.

FBI iDSM will send the message to DHS iDSM (CIMS to VIPS).

EBTS records coming from US-VISIT will include Subject Name, Image, Date of Birth, and Gender.

The FBI_Hit_Notification_Request element will map to the Input portion of the WHit_RQS_WS_VIPS Web Service.

- Inputs into the web service call will conform to the fields listed within the FBI_Hit_Notification_Request element of the XSD.

The FBI_Hit_Notification_Response element will map to the Output portion of the WHit_RQS_WS_VIPS Web Service.

- Outputs that result from the web service call will produce data that conforms to the fields listed within the FBI_Hit_Notification_Response element of the XSD.

I.2.6 DHS_Hit_RQS_CIPS XSD

This represents a Want and Warrant Hit Notification Web Service Request as well as its corresponding Web Service Acknowledgement Response.

DHS iDSM will send the message to FBI iDSM (VIMS to CIPS).

The DHS_Hit_Notification_Request element will map to the Input portion of the WHit_RQS_WS_CIPS Web Service.

- Inputs into the web service call will conform to the fields listed within the

DHS_Hit_Notification_Request element of the XSD.

The DHS_Hit_Notification_Response element will map to the Output portion of the WHit_RQS_WS_CIPS Web Service.

– Outputs that result from the web service call will produce data that conforms to the fields listed within the DHS_Hit_Notification_Response element of the XSD.

I.2.7 FBI_Image_RQS_VIMS XSD

This represents an FBI Image Web Service Request as well as its corresponding Web Service Acknowledgement Response.

FBI iDSM will send the message to DHS iDSM (CIPS to VIMS).

EBTS records coming from FBI will include Subject Name, Image, Date of Birth, and Gender.

The FBI_Image_Request element will map to the Input portion of the WBio_RQS_WS_VIMS Web Service.

– Inputs into the web service call will conform to the fields listed within the FBI_Image_Request element of the XSD.

The FBI_Image_Response element will map to the Output portion of the WBio_RQS_WS_VIMS Web Service.

– Outputs that result from the web service call will produce data that conforms to the fields listed within the FBI_Image_Response element of the XSD.

I.2.8 DHS_Image_RQS_CIMS XSD

Represents a DHS Image Web Service Request as well as its corresponding Web Service Acknowledgement Response

The DHS_Image_Request element will map to the Input portion of the WBio_RQS_WS_CIMS Web Service.

– Inputs into the web service call will conform to the fields listed within the DHS_Image_Request element of the XSD.

The DHS_Image_Response element will map to the Output portion of the WBio_RQS_WS_CIMS Web Service.

– Outputs that result from the web service call will produce data that conforms to the fields listed within the DHS_Image_Response element of the XSD.

APPENDIX J CJIS ESAN

J.1 Introduction

The CJIS Enterprise Storage Area Network (ESAN) segment currently provides storage to the majority of CJIS business units / segments. This storage is primarily of the tier-1 class storage constituted of SCSI drives or Logical Unit Numbers (LUNs). The primary interface to this storage is Fibre Channel. Enhancements to the ESAN segment detailed herein intend to provide additional classes of storage, as well as other interfaces to said storage. These additional classes of storage and interfaces intend to provide storage services, to existing and upcoming CJIS segments, which are more appropriate concerning data store requirements, as well as decrease coupling and increase cohesion concerning the relationship between an ESAN user segment and the ESAN segment.

The primary application of the Celerra/Centera tier-2 storage hardware is to receive and store palm prints, photos, irises and supplemental fingerprint/palm prints according to ANSI/NIST standards. When the FBI Electronic Biometric Transmission Specification (EBTS) (version 8.1) document is formally accepted, the acceptance of all photo, iris, palm print, supplemental finger/palm print, or the new Type-99 for novel biometric information can begin almost immediately if submitted as an additional record type to a fingerprint transaction.

J.2 Segment Overview

The enhancements for the ESAN segment are delivered via the following products / solutions:

- EMC Celerra
- EMC Centera
    - EMC Centera Universal Access
- EMC DiskXtender
- ESAN Service Portal Server

J.2.1 Celerra

The Celerra NSX gateway product is a Network Attached Storage (NAS) server which primarily provides storage access to host systems via NFS and CIFS share interfaces. The actual storage for these shares is provided to the Celerra via the existing ESAN DMXs.

J.2.1.1 Celerra NSX system Elements

The Celerra NSX provides a highly available cluster of dedicated file server blades, called X-Blades or data movers, connected to a Fibre Channel SAN, and managed by a single point of control, the control station. The control station is actually a redundant pair of servers operating in an active-passive configuration. Blades are autonomous file servers providing clients with support for NFS, CIFS, iSCSI over optical 10 Gigabit, optical and multiple copper Gigabit Ethernet connections. Celerra's X-Blade operating system, DART, is optimized for high performance network file access. This real-time, embedded operating system runs on each X-Blade to increase performance, simplify management and scale linearly to accommodate large user communities. The ESAN configuration consists of 6 active X-Blades and 2 standby X-Blades per NSX cabinet.

J.2.3 Centera

The EMC Centera is a Content Addressed Storage (CAS) system. Traditional SAN attached storage systems provide storage via the presentation of SCSI disks or targets, with block level data access. Traditional NAS storage systems provide storage via the presentation of network shares and file level access. The Centera CAS system provides storage as an appliance on an IP network, which accepts objects and metadata sent via a socket connection and returns a content address / C-Clip, for said objects. This content address combined with the presentation of an authorization file PEA file (essentially a shared private key) acts as a claim check to the data that has been stored. Centera CAS storage is not able to be accessed as quickly as teir-1 Fibre Channel based storage, such as in the ESAN DMXs, however it is meant to be a long term archive of data that infrequently changes.

J.2.4 DiskXtender

The ESAN segment will deploy the EMC DiskXtender for NAS software component. The DiskXtender File System Manager for NAS (DX-NAS) is an archiving solution that allows the user to free storage space on the NAS server while maintaining NAS client access to archived files. The solution consists of integrating the following three components:

- An EMC Celerra
- The DX-NAS policy engine
- Secondary storage. In this case EMC Centera

Again, EMC DiskXtender for NAS is a software application.

J.3 Solution

The storage enhancements to the ESAN system that have been mentioned so far, were selected to initially provide a solution for migrating the existing EFCON AIT tape library data to a storage class more appropriate for the access nature of the data.

Specifically the "efs" servers will mount storage via NFS hosted on the Celerra NSXs; the DiskXtender application running on an ESAN Windows host will also have access to these network shares; the DiskXtender application will, by policy, transparently and non-disruptively migrate the data from the NSXs to the Centera storage platform. The data will still be visible as though it was stored on the Celerra but will actually reside on the Centera.

From an ESAN perspective, the addition on the Celerra, DiskXtender and Centera components represent the following changes to ESAN storage services:

J.3.1 Centera

- Addition of an "*archive*" tier of storage
- Addition of an *interface* to storage which can be natively integrated into a host application without the construct of disks or filesystems on the application host
- Addition of a storage service which can mathematically prove that the data returned was what was stored on a bit by bit basis
- Addition of the capability to enforce retention periods on data, as dictated by policy, regardless of instruction by a host application to delete a given unit of data

J.3.2 Centera Universal Access (CUA)

- Addition of the CUA server is a direct NFS and CIFS interface to Centera storage.
- The CUA service differs from the Celerra-DiskXtender-Centera solution in that the CUA is suited to smaller, simpler workloads, and does not intend to leave any data on local filesystem share, but archives all data to Centera within 1 minute of ingest.

J.3.3 Celerra

- Addition of highly available NFS, CIFS, FTP, HTTP, SMB, MPFS, iSCSI interfaces to the same storage infrastructure (DMXs) currently used by the ESAN environment

- Addition of NFS, CIFS, iSCSI interfaces which can present a given size device or amount of storage but in reality be an amount much smaller and grow their actual size dynamically

J.3.4 DiskXtender

- Addition of the capability to non-disruptively and transparently migrate data between storage tiers

J.4 Monitoring and Management Information

J.4.1 Centera

- Monitoring the Centera infrastructure is completely integrated with the existing ESAN ECC infrastructure
- Management access to the Centera does not allow access to the data stored on the Centera
- Management access to the Centera is provided via a client application "Centera Viewer" and "Centera Console"
- I/A for applications that will use the Centera storage is achieved via a PEA file. This file is generated on the Centera, associated with a give access profile and a given storage pool. The file is then copied to the host accessing the Centera and submitted to the Centera when storing or retrieving data.
- Centera Governance edition is enabled which means audited deletions are enabled and existing retention period may be dynamically changed.

J.4.2 CUA

- The CUA server is a Linux based operating system installed on a Dell 2850 server.
- The CUA can be accessed via GUI front end at https://address:7227 as well as ssh version 2.
- The CUA server should be viewed as an appliance as its feature set and capabilities, both from security and a storage perspectives, are limited.
- Identification and Authentication to the CUA server for monitoring and administration are only in the form of factory default accounts.
- The CUA server will email health related problems and notice of backup / restore completion, as well as the Content Addresses that have been backed up to the ESAN ESP "esanalerts" SMTP address.
- Much like the Centera access nodes, the CUA server only resides on the CENTERA-ARCHIVE VLAN.

J.4.3 Celerra

- The X-Blades of the Celerra NSXs or data movers are not capable of being logged into remotely in any way.
- Monitoring of the Celerra NSXs is achieved via the ESAN ECC application.

- Management of the Celerra NSXs is achieved either through secure http connection to the active NSX control station where access to a gui is provided; or through direct ssh access to the NSX control station where command line functionality controls the appliance
- I/A for management access via the NSX control station is achieved to a local account on the control station
- Celerra NSX blades utilize existing ESAN DNS and NTP services
- In a multi-protocol file sharing situation (i.e. the same file share is presented via both CIFS and NFS), a local password and group file on each blade contains the CIFS to NFS uid and gid mapping ensuring a user with an account in both environments maintain the appropriate file access
- Presented CIFS shares are made available via virtual CIFS server which must join the appropriate windows domain for CIFS access from that domain
- CIFS shares and their associated virtual servers, which will be presented to the DiskXtender host for archival of data, are part of the ESAN domain

J.4.4 DiskXtender

- The DiskXtender application runs on an ESAN Windows host, which is part of the ESAN domain (residing in the Member Servers: Cluster Server OU)and has applicable GPOs applied in accordance with existing ESAN practices
- Monitoring and Management of the DiskXtender application is achieved via the DiskXtender Client application which requires an I/A process specific to the application and not part of the domain.
- The user which runs the DiskXtender windows services must be a domain account with permission to read and write data to the shares that it will act upon.

J.5 Hardware Diagram

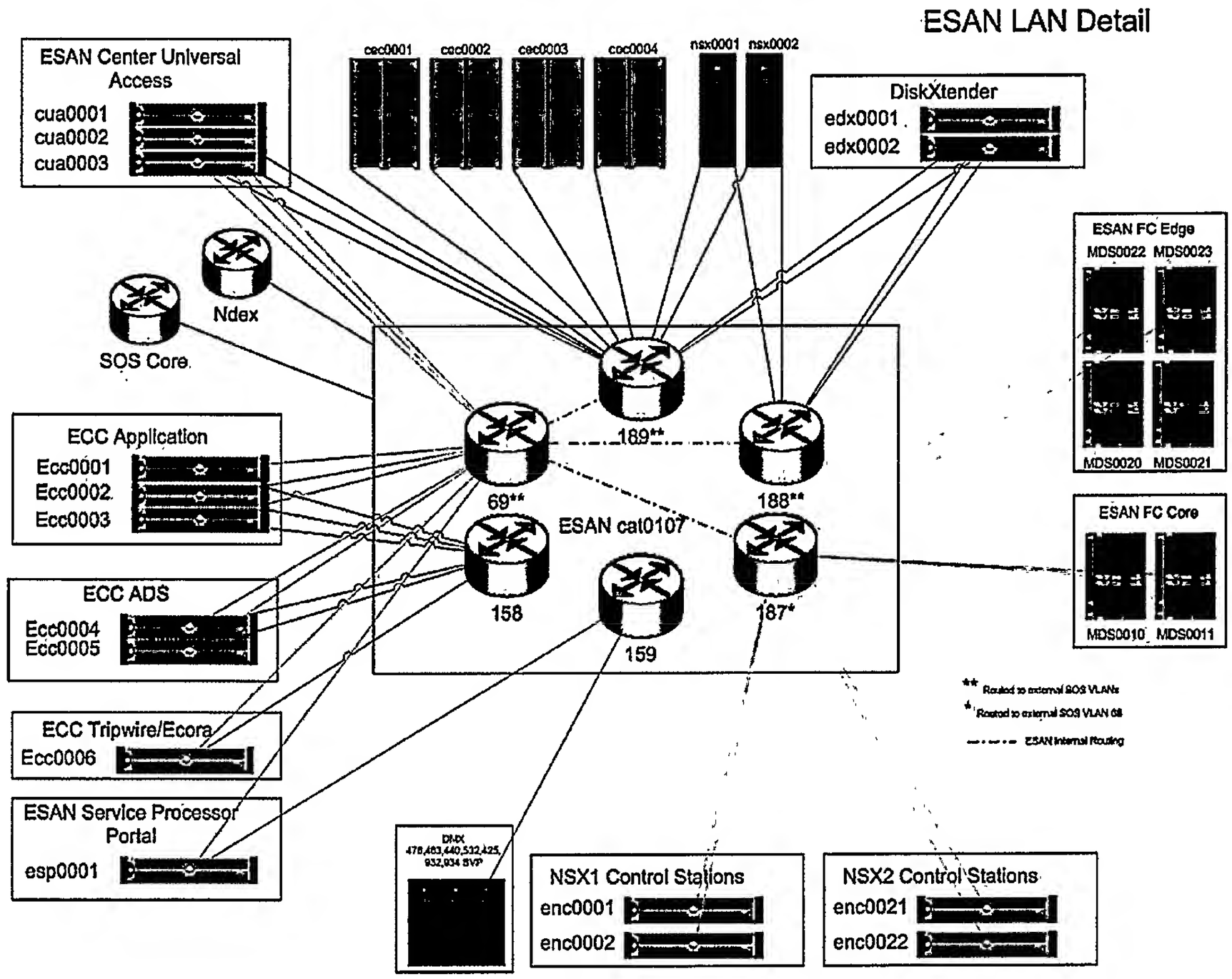


Figure J.5.1 Hardware Diagram

J.6 Data Flow

This section intends to describe data flow concerning the applicable components of the enhancements to the ESAN segment. It then provides a consolidated data flow description of the Celerra-DiskXtender-Centera solution.

J.6.1 Centera Data Flow

Data transfer to and from Centera is as follows. A host either on the ESAN network or with access to the ESAN-CENTERA-ARCHIVE VLAN(189) opens a connection to Centera, identifies and authenticates, and writes or reads data. Identification and authentication occurs via one

of two methods: via access profile name and password or via PEA file.

J.6.2 Access Profile Name and Password

During this identification and authentication method the host system supplies an access profile name which has been preconfigured on the Centera unit. Access profiles define the level of access or role to the Centera Cluster, as well as what storage pool or pools are available to that access profile. All host applications which will store and retrieve data from the ESAN Centera storage will have a predefined access profile granting only read and write operations on their associated pool. After the access profile name have been given, then a preconfigured password for that access profile must be submitted. After successful verification of the password then the associated host is granted a connection.

J.6.3 PEA file I/A

A PEA file is a Centera generated file that contains the applicable access profile name as well as a private key. For every host system / application using this method to connect to the Centera storage a PEA file will be generated on the applicable Centera unit(s). This file will then be given to the application owner for use.

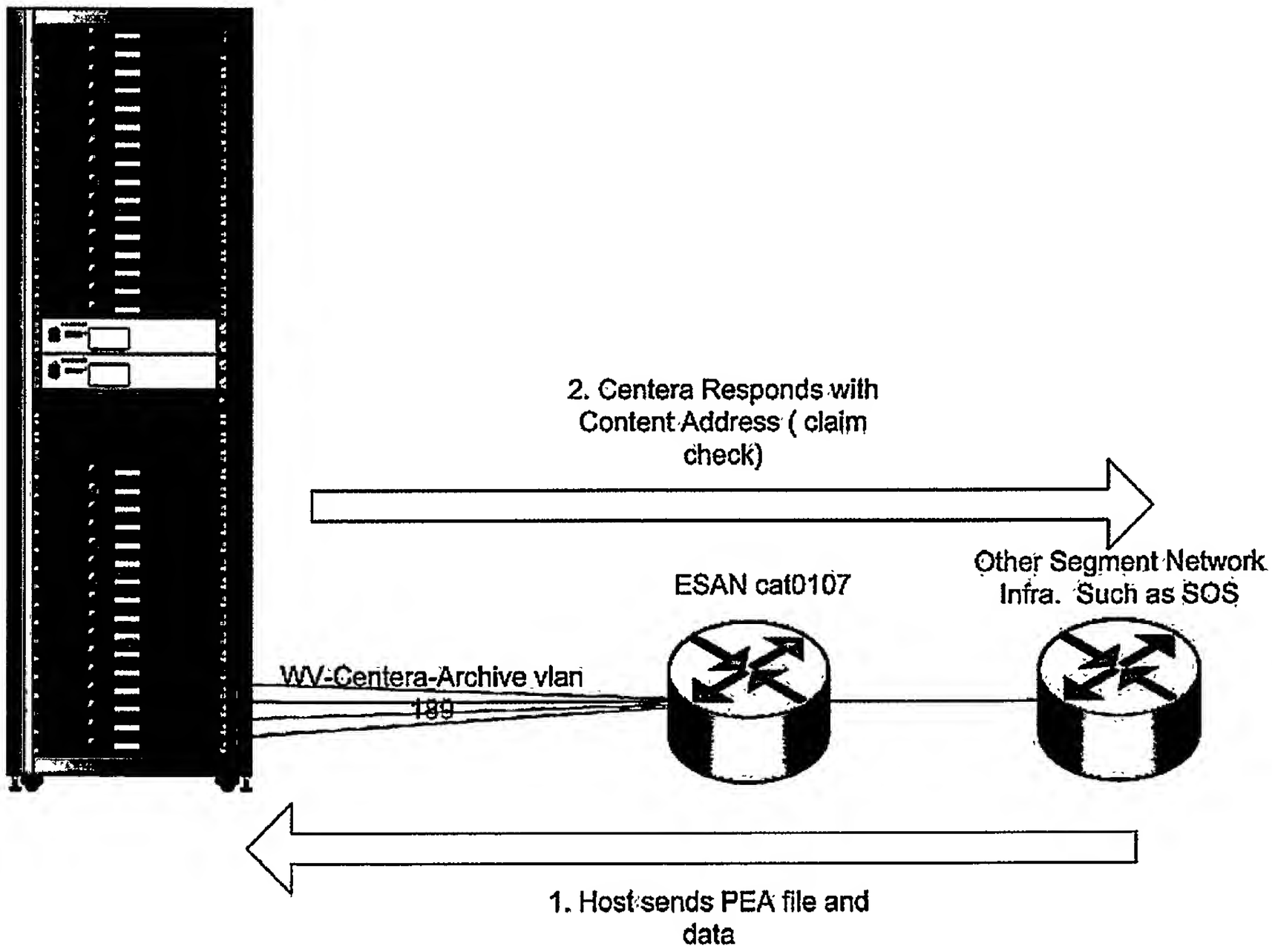


Figure J.6.3.1 PEA file I/A

J.6.4 Celerra Data Flow

Data flow into and out of the Celerra storage interfaces occurs via ESAN-CELERRA-DATA VLAN (188). Security mechanisms associated with Celerra NSX data flow are that of NFSv1, NFSv2, NFSv3 and CIFS.

J.6.5 NFS

By policy, for a given NSX NFS share, only the IP addresses or networks requiring access will be allowed access to said share(s). Also, only those hosts requiring NFS share root privileges will be allowed said access to their applicable shares.

J.6.6 CIFS Active Directory Integration

For the CIFS protocol, a virtual CIFS server is created on the NSX for the systems domain that requires access to the applicable CIFS share. This CIFS server is joined to the domain in question.

J.6.7 Multi-Protocol File Sharing

For the implementations which require multi-protocol file sharing (such as the EFCON AIT Library replacement) a local password and group file is created on every blade (with applicable share(s)) which translates the UID,GID to SID mapping such that should the same user exist in the CIFS domain and NFS domains, the correct file permissions are maintained.

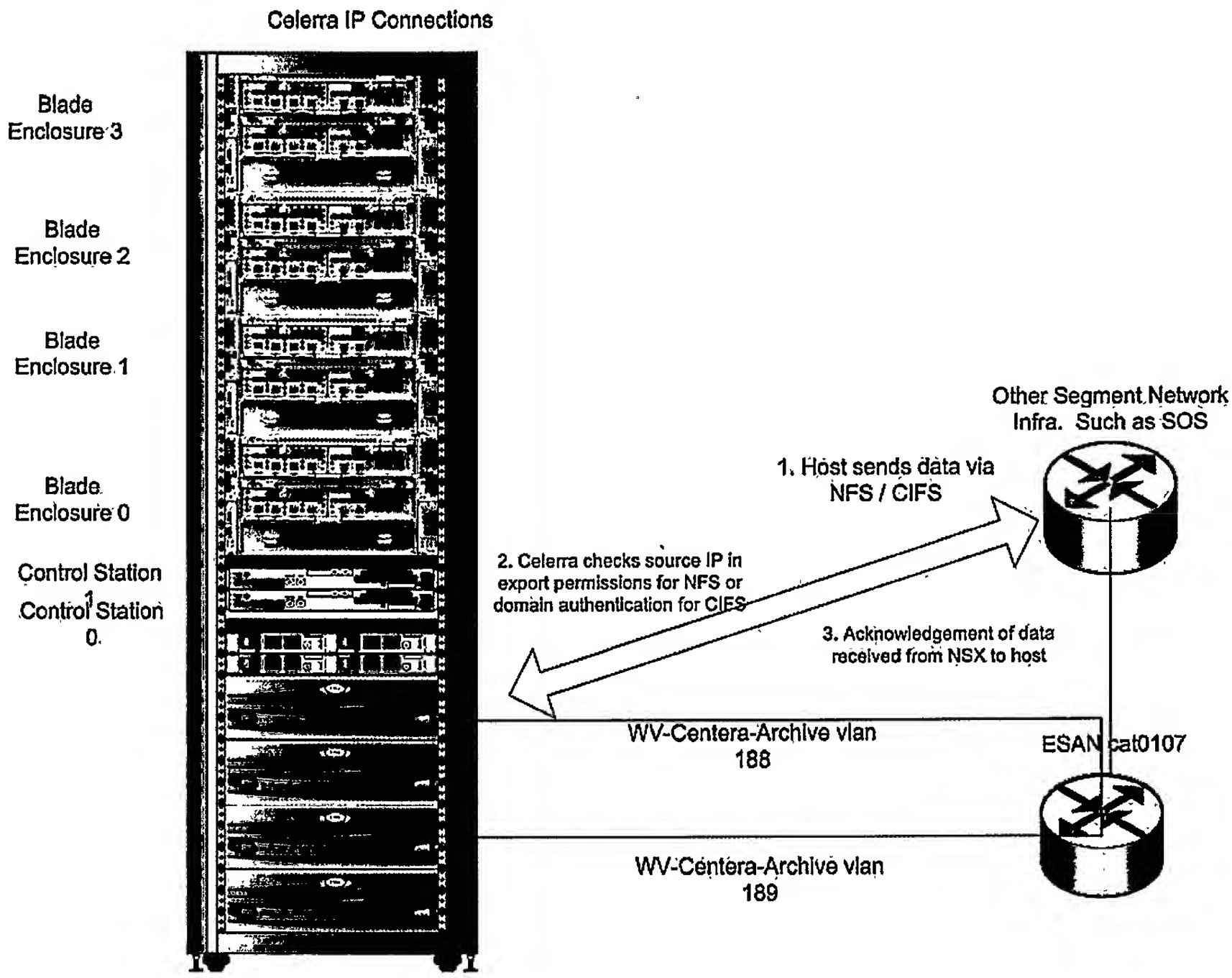


Figure J.6.7.1 Multi-Protocol File Sharing

J.6.8 Integrated DiskXtender (DX) Data Flow

The following descriptions and diagrams are intended to overview the data flow as it relates to the DiskXtender application. Because DiskXtender is an application integrated with sources (Celerra NSX files shares) and destinations (Centera) is necessary to explain DiskXtender operations as they relate to Celerra and Centera.

J.6.8.1 DX Data Flow – Step 1

DX maintains the construct of sources, destinations, policies, jobs and schedules. The following is explained as it relates for the ESAN implementation. Further functionality of DX is available but it is outside the scope of the ESAN implementation.

- Sources are file shares what are visible to the DX server. Sources must be readable and writable by the DX server.
- Destinations are the EMC Centera in the ESAN implementation.
- Policies are actions that the DX server will execute against the source and / or destination such as migrating data, looking for orphaned files on the source, or scanning the destination for orphaned objects.
- Jobs are the instantiation of policies.
- Schedules are mechanisms for automatic repeated executions of jobs.

The first step depicted in the following diagram intends to show that for the execution of a given migration job the DX server scans the source filesystems based on the criterion specified in the applicable policy. After a file is identified for migration (and while other files are being identified or searched for) the DX server communicates to the Celerra NSX via the Celerra FileMover API and instructs the Celerra NSX to migrate the data region of said file to a pre-configured destination.

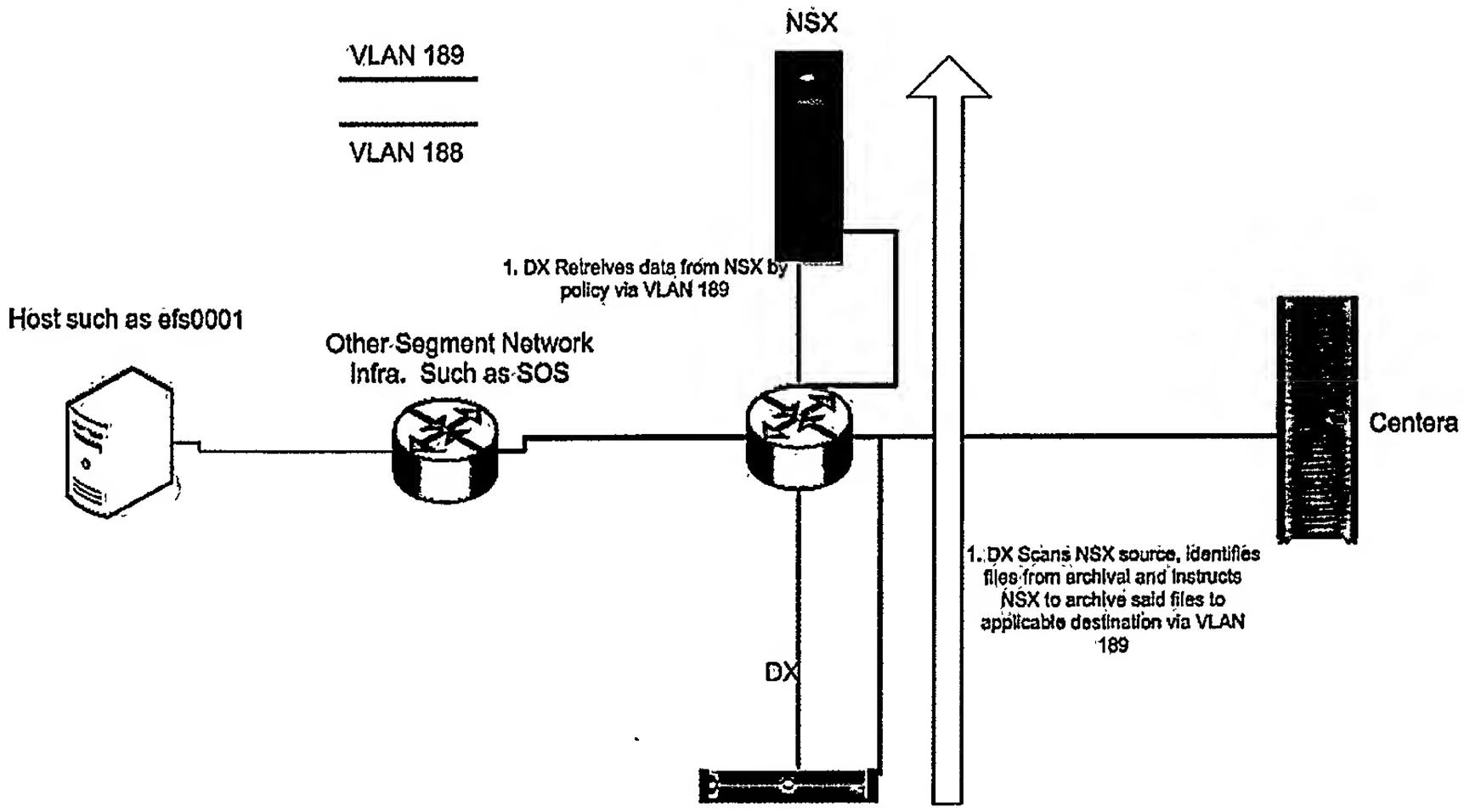


Figure J.6.8.1.1 DX Data Flow – Step 1

J.6.8.2 DX Data Flow – Step 2

In the case of the ESAN implementation, the applicable destination is an http server on the DX server which then interfaces with Centera via the Centera API. In other words, for the data to be migrated, the transport protocol is HTTP to the DX server which calls certain CGI routines on the DX server, thereby writing the data to Centera. HTTPS is not available for this transport.

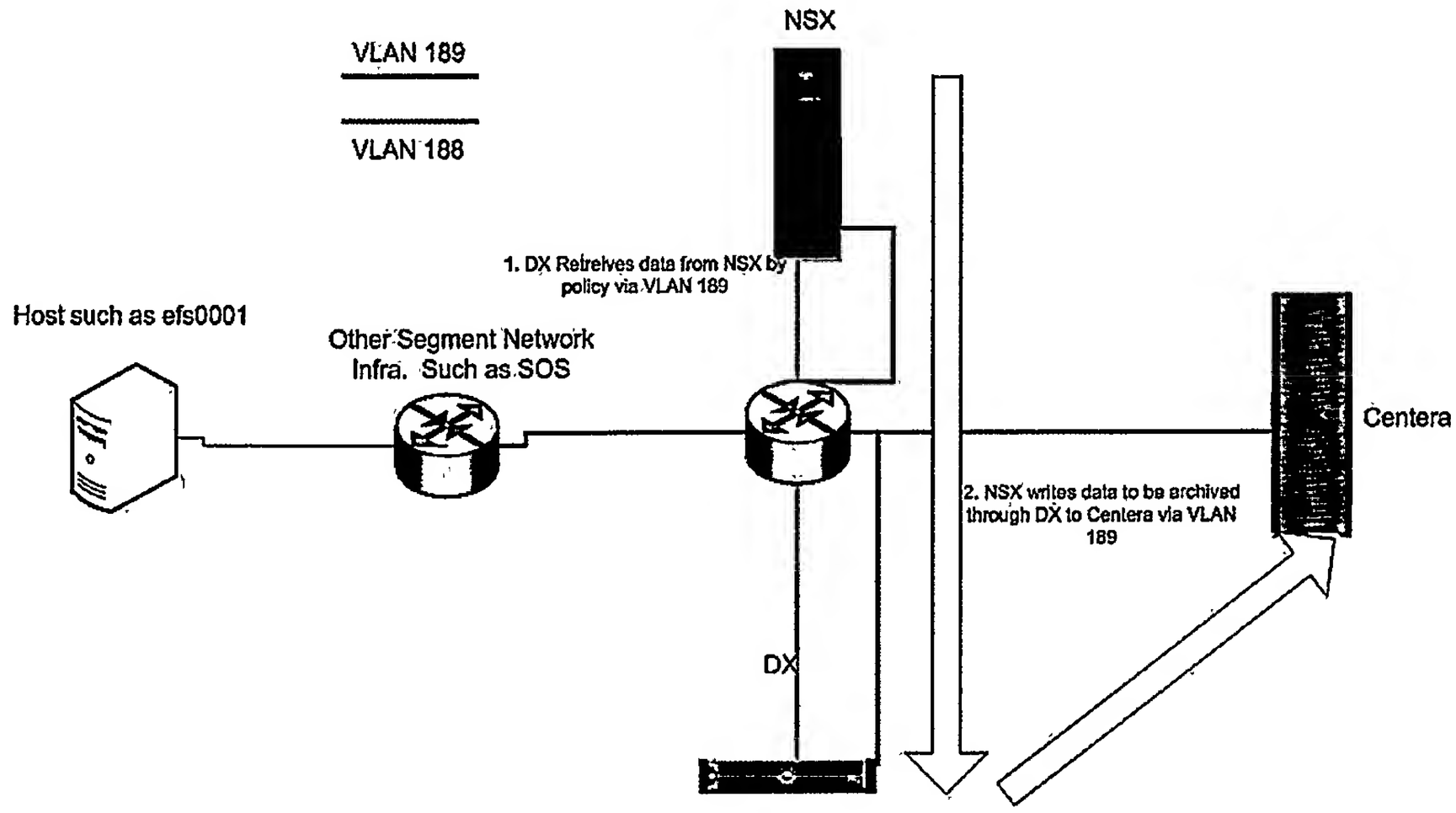


Figure J.6.8.2.1 DX Data Flow – Step 2

J.6.8.3 DX Data Flow – Step 3

For the final step of the file migration, the Centera returns the C-Clip metadata in xml format to the DX server along with the calculated md5 based Content Address (CA). The DX server stores this C-Clip metadata in a local proprietary (pgsql based) database with other information regarding the migration for said file. Then the DX server returns the CA to the Celerra, where the Celerra replaces the original file with a "stub" file containing the destination, CA and other pertinent information.

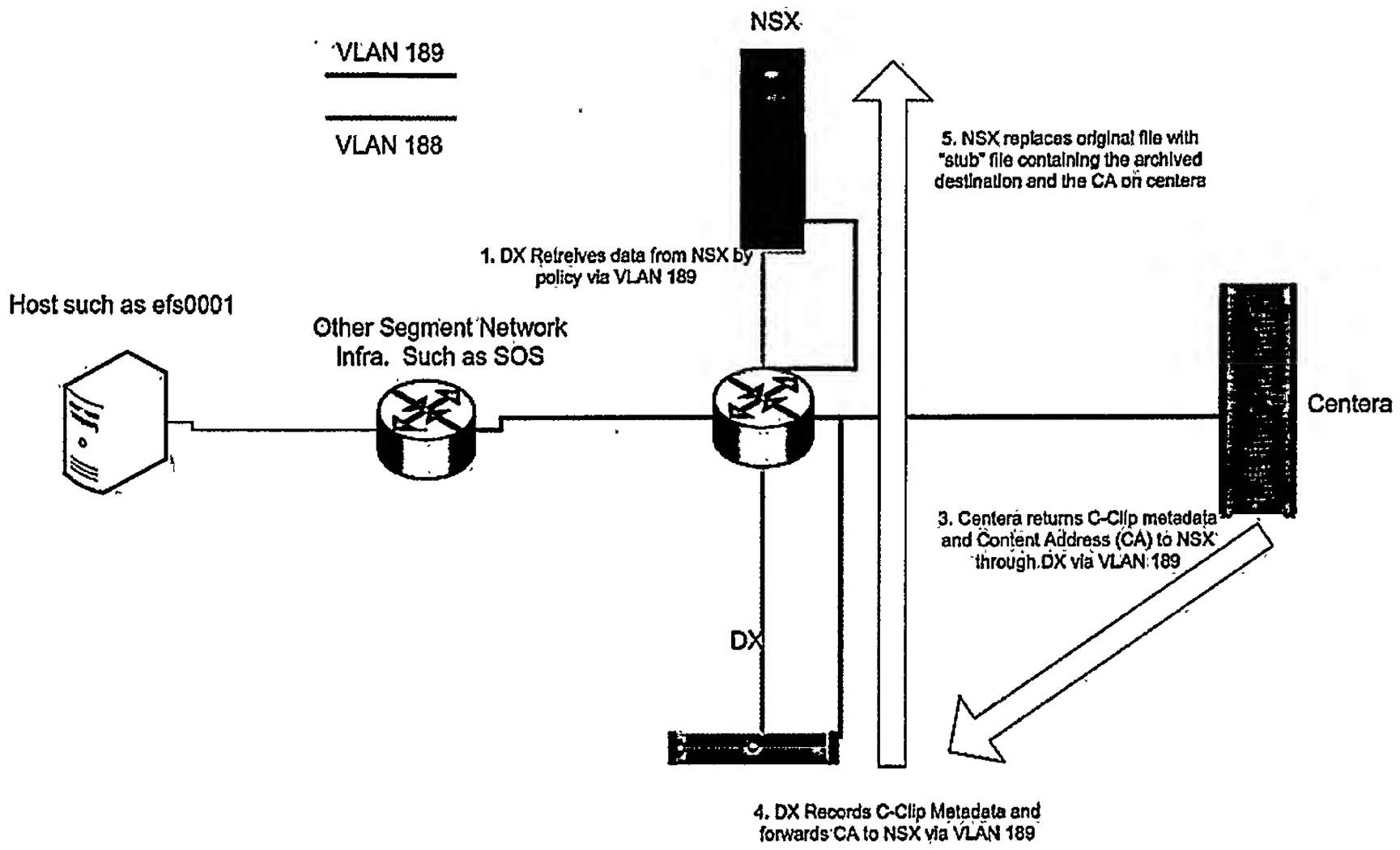


Figure J.6.8.3.1 DX Data Flow – Step 3

J.7 Solution Infrastructure Services Flow (Examples)

Certain infrastructure protocols are common to some or all of the aforementioned ESAN enhancements. These common protocols and services are NTP, DNS, and, in some cases, ADS.

J.7.1 NTP

The following components utilize NTP time synchronization via the ESAN Catalyst switches / routers:

- Celerra
- Centera
- DiskXtender Server (via ADS integration)
- CUA
- Service Processor Portal

J.7.2 DNS

The following components utilize DNS time synchronization via the ESAN Domain controllers /

DNS servers

- Celerra
- Centera
- DiskXtender Server (via ADS integration)
- CUA
- Service Processor Portal (via ADS integration)

J.7.3 ADS

The following components are integrated as members of the ESAN domain noe.cjis.fbi.gov / oe.cjis.fbi.gov:

- Celerra
  - Virtual Data Movers / Virtual CIFS servers join the ESAN domain (no applicable GPOs)
- DiskXtender Server
- Service Processor Portal

J.8 Monitoring

J.8.1 Monitoring – Centera

Basic monitoring of the Centera clusters is accomplished via the ECC Storage agent for Centera. Monitoring capabilities include all health and wellness attributes of the Centera systems.

Enhanced monitoring the Centera Clusters is via the Centera Console application. This application will be installed on its own server in the ESAN environment, it also maintains the capability to monitor the log of successful and unsuccessful logins, both by application and administrator (in the Centera environment that are really the same), monitor performance, view alert and command history.

J.8.2 Monitoring – Celerra

Monitoring of the Celerra NSXs is accomplished via the ECC Storage agent for NAS. Monitoring capabilities include all health and wellness attributes of the Celerra systems.

J.8.3 Monitoring – DiskXtender

Monitoring of the DiskXtender server is accomplished via the ECC Host Agent for Windows. Monitoring capabilities include all health and wellness attributes of the DiskXtender host system.

Monitoring of the DiskXtender application is accomplished via the DX for NAS GUI. This interface is installed on the applicable DX servers. Login to this application requires the authorization to launch the application via ADS GPOs, as well as an additional username and password that is stored in the local DX database.

J.9 Administration

J.9.1 Administration – Centera

Administration and changes to the Centera clusters are accomplished via the Centera Viewer application, installed on the ESAN workstations, or ssh version 2 access to the Centera access nodes. Access to the Centera Viewer application is managed by ADS GPOs. After the Centera Viewer application is started, access to a Centera cluster is accomplished by providing an access profile name (in the form of a username) and a secret which is locally stored on the Centera. The access profile name provided must have at least the Monitoring role associated with it.

J.9.2 Administration – Celerra

Administration of the Celerra NSXs is accomplished via access to the Celerra Control Station. Network administration access (via ssh, or via https) to the Celerra control station is limited to the built-in "nasadmin" account. After accessing the nasadmin account, the Celerra is administered via multiple commands that may act upon the control station, and/or one or more X-Blades. Elevation to root privileges is seldom required but may be garnered after logging in via the network as the nasadmin user.

J.9.3 Administration – DiskXtender

Administration of the DiskXtender server follows the standard administration of the windows domain.

Administration of the DiskXtender application accomplished via the DX for NAS GUI. This interface is installed on the applicable DX servers. Login to this application requires the authorization to launch the application via ADS GPOs, as well as an additional username and password that is stored in the local DX database

J.10 Ports and Services

J.10.1 Ports – Celerra

Table J.10.1 Ports – Celerra

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
20	TCP	Open	FTP	Yes	Port used for FTP data Transfers. This may be disabled be disabling FTP as described below. Authentication is performed on port 21 and defined by the FTP protocol.
21	TCP	Open	FTP	Yes	Port 21 is th control port on which the FTP service listens for incoming FTP requests. The authentication process is defined by the FTP protocol definition and cannot be changed. It is possible to authenticate using either Unix names or a Windows domain and user name (domain\user). By default, all Data Movers Run the FTP service and this port is active. If the FTP service is not desired, it may be disabled by using the following procedure: • Disable FTP on the Data Mover o Use vi to edit the file `/nas/server/<server_name>/netd` • Comment out the ftpd line o Ftpd becomes #ftpd • Restart the Data Mover o This may me reset automatically during an upgrade, be sure to recheck Details on running and managing the FTP service on a Data Mover is documented in the EMC Technical Module *Using FTP on Celerra Network Server*.
69	UDP	Open	TFTP	Yes	Initially TFTP listens on UDP port 69. After a request is read on port 69, a different port is ran-

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
					domly chosen to use for the TFTP data transfer. By definition, TFTP does not authenticate requests. The TFTP service is not started by default, it must be manually started. TFTP operation, including how to disable the service, is documented in the EMC Technical Module *Using TFTP on Celerra Network Server*.
111	TCP/UDP	Open	rpcbind (Network Infrastructure)	No	This port is opened by the standard port mapper or rcpbind service and is an auxiliary Celerra network service. It cannot be stopped. By definition, if a client system has network connectivity to the port, they may query it. No authentication is performed.
137	UDP	Open	NETBIOS Name Service (CIFS)	Yes	The NETBIOS Name Service is associated with the Celerra's CIFS file sharing services and is a core component of that feature. This port may be disabled by not offering CIFS services. If CIDS services are enabled, this port is active. It is specifically required for older versions of the Windows OS (Pre-Windows 20000). There is no authentication, in accordance with Microsoft standards. Clients with legitimate access to the Celerra's CIFS services must have network connectivity to the port for continued operation. This port can be closed by running the command `server_setup server_d -P -o cifs -stop`. Note that this disables all CIFS-related services.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
138	UDP	Open	NETBIOS Datagram Service (CIFS)		The NETBIOS Datagram Service is associated with the Celerra's CIFS file sharing services and is a core component of that feature. This port may be disabled by not offering CIFS services. If CIDS services are enabled, this port is active. It is specifically required for older versions of the Windows OS (Pre-Windows 20000). There is no authentication, in accordance with Microsoft standards. Clients with legitimate access to the Celerra's CIFS services must have network connectivity to the port for continued operation. This port can be closed by running the command `server_setup server_d -P -o cifs -stop`. Note that this disables all CIFS-related services.
139	UDP	Open	NETBIOS Session Service	Yes	The NETBIOS Session Service is associated with the Celerra's CIFS file sharing services and is a core component of that feature. This port may be disabled by not offering CIFS services. If CIDS services are enabled, this port is active. It is specifically required for older versions of the Windows OS (Pre-Windows 20000). There is no authentication, in accordance with Microsoft standards. Clients with legitimate access to the Celerra's CIFS services must have network connectivity to the port for continued operation. This port can be closed by running the command `server_setup server_d -P -o cifs -stop`. Note that this disables all CIFS-related services.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
161	UDP	Open	SNMP (Management Infrastructure)	Yes, with loss of functionality	The Simple Network management Protocol (SNMP) is a management and monitoring service used by many third party management tools. The Data Mover uses SNMP, version 1 as defined by RFC 1157. This version of SNMP does not support modifying any of the monitored values. Authentication is based upon a client system knowing the community string. The community string is "public" by default and should be changed using the `server_snmp` command. SNMP is used for come communication between the Control Station and the Data Mover, if it is disabled, the `server_netstat` command will cease to function properly. Instructions for disabling the SNMP service on a Data Mover are defined in the Primus solution emc61038.
445	TCP	Open	CIFS	Yes	This port is the new default CIFS connectivity port for Windows 2000 and later clients. This port is disabled by not offering CIFS services. If CIFS services are disabled, then this port is inactive. Authentication is addressed on this port in accordance with Microsoft practices (de facto standards). Clients with legitimate access to the Celerra's CIFS services must have network connectivity to the ports for continued operation. CIFS services can be closed by running the command `server_setup server_d -P -o cifs -stop`. Note that this disables all CIFS-related services.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
520	UDP	Open	Routing Information Protocol (RIP)	Yes	Routing Information Protocol (RIP): A routing protocol optimized for creating routed within one organization (interior gateway protocol). RIP is a distance-vector protocol that used hop count (max 15) as the metric. RIP-1 does not send the mask in updates. RIP-2 sends the mask in updates. [From: EMC Technical Module Configuring and Managing Celerra Networking] This technical module explains the purpose and configuration of RIP services on the Data Mover. Instructions for disabling the service are included.
1234	TCP/UDP	Open	mount (NFS)	No	The mount service is a core component of the NFS service (versions 2 and 3) and is an important component of Control Station to Data Mover interaction, even if there are no NFS exports externally visible from the Data Mover. There are several methods of controlling access to NFS exports and these are described in the EMC Technical Module *Managing NFS Access to the Celerra Network Server*. Authentication of users is AUTH_SYS be default. If stronger authentication is desired, Secure NFS is available as an RPQ item. Secure NFS provides Kerberos authentication for end users. Clients with legitimate access to the Celerra's NFS services must have network connectivity to the port for continued operation.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
2049	TCP/UDP	Open	NFS	No	This port is used to provide NFS services and is an important part of the Control Station to Data Mover interaction, even if these are no NFS exports externally visible from the Data Mover. There are several methods of controlling access to NFS exports and these are described in the EMC Technical Module *Managing NFS Access to the Celerra Network Server*. Authentication of users is AUTH_SYS be default. If stronger authentication is desired, Secure NFS is available as an RPQ item. Secure NFS provides Kerberos authentication for end users. Clients with legitimate access to the Celerra's NFS services must have network connectivity to the port for continued operation.
4647	UDP	Open	lockd forward (Infrastructure for NFS Cluster)	Yes	This is not a public service. It is used only on the Celerra interconnection network. External clients will not need to reach this service. It may be blocked by a firewall. This service is used by the DART NFS Cluster product. To determine if any NFS clusters are configured, use the command `nas_server -l`. The cluster will have the type "group". To remove any NFS clusters use the command `nas_server clster_name -delete`.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
4658	TCP	Open	Protable Archive Interchange (PAX) (Network Infrastructure)	Yes	Portable Archive Interchange (PAX): A Celerra Network Server archive protocol that works with standard UNIX tape formats. The protocol is used only between the Control Station and Data Mover. It is only used on the private network. This service may be disabled if the local tape backup is not used. Details on how to disable this service are in Primus under ID emc49339. Background information on PAX is contained in the relevant EMC documentation on backups and NDMP. There are several technical modules on this topic to seal with a variety of backup tools.
5033	TCP	Open	NBS (Network Block Service)	No	An EMC proprietary protocol similar to (and a precursor of) iSCSI. Externally, NBS is used for control types of functions in the area of smap, replication, and iSCSI management. CHAP authentications are required to establish an NBS connection. On NS platforms, NBS is always started (port opened and listened to) to provide control station access to the back-end. On the CNS platform, NBS is started by the iSCSI service. This port can be placed behind a firewall. The NBS service that opens this port is a core Celerra service and cannot be stopped. This is not a "public" service. When used for Control Station to Data Mover communication it is only used on the private Celerra interconnection network. Clients will not need to reach this service.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
5080	TCP	Open	HTTP (FileMover support & infrastructure)	Yes	HTTP is used as a transport mechanism for FileMover and for some Control Station to Data Mover information exchanges. FILEMOVER traffic is for ILM-related policy engines to send commands to the Data Mover. The policy engines are authenticated using the HTTP digest authentication method. This is described in the FILEMOVER documentation. See EMC Technical Module *Configuring DHSM on Celerra* for configuration and monitoring commands. HTTPS (HTTP over SSL) is not currently available on the Data Mover. Because the HTTP transport is also used for Control Station to Data mover interactions, the service may not be disabled. However, this only requires that HTTP requests be accepted from the Control Station by the Data Mover over the private network within the Celerra cabinet. Access to the HTTP service by external agents is disabled by default.
8888	TCP	Open	RCP (Replication Services)	Yes	This port is used by the replicator (on the secondary side). It is left open by the replicator as soon as some rate has to be replicated. Clients (other Celerra servers) using the replication service must be behind the same firewall for continued operation.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
10000	TCP	Open	NDMP (Backup Services)	Yes	The Network Data Management Protocol (NDMP) allows you to control the backup and recovery of an NDMP server through a network backup application, without installing third-party software on the server. In a Celerra Network Server, the Data Mover functions as the NDMP server. The NDMP service can be disabled if the NDMP tape backup is not used. The NDMP service is authenticated with a username/password pair. The username is required to be "ndmp" for Celerra 5.3 and earlier releases, and configurable from 5.4 and later releases. The NDMP documentation describes how to configure the password for a variety of environments.
12345	TCP	Open	usermapper (CIFS)	Yes	The usermapper service is associated with the Celerra's CIFS services. This is the method by which Windows credentials (which are SID-based) are mapped to UID and GID values. This port can be placed behind a firewall. The service that opens this port is usermapper and is a core Celerra service. It cannot be stopped.
31491	UDP	Open	RFA (Remote File Access) NFS Functionality	Yes	The service that opens this port is RFA and is a core Celerra service associated with NFS. It cannot be stopped.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
38914	UDP	Open	nfs forward (Infrastructure for NFS Cluster)	Yes	This is not a public service. It is used only on the Celerra interconnection network. External clients will not need to reach this service. It may be blocked by a firewall. This service is used by the DARD NFS Cluster product. To determine if any NFS Clusters are configured, use the command `nas_server -l`. The cluster will have the type "group". To remove any NFS clusters use the command `nas_server cluster_name -delete`.
49152 thru 65535	TCP/UDP	Open	Statd NFS Support	Yes	statd is the NFS file-cocking status monitor and works in conjunction with lockd to provide crash and recovery functions for NFS (which is inherently a stateless protocol). statd is a core service but it can be stopped. Clients with legitimate access to the Celerra's NFS services would need to have network connectivity to this port.
49152 thru 65535	TCP/UDP	Open	rquotad Quota Support	Yes	The rquotad daemon provides quota information to NFS clients who have mounted a file system. An NFS user that has mounted a Celerra file system can access quota information for the file system using the quota command. This command runs on the client side and interrogates the rquotad daemon on the Data Mover via RPC. To use this functionality, the client must have already mounted the file system. Authentication is AUTH_SYS, the same as is used for the NFS protocol. You must have root access to the file system to get the quota information for different users.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
49152 thru 65535	TCP/UDP	Open	Lockd NFS Support	Yes	lockd is the NFS file-cocking status monitor and works in conjunction with statd to provide crash and recovery functions for NFS (which is inherently a stateless protocol). lockd is a core service but it can be stopped. Clients with legitimate access to the Celerra's NFS services would need to have network connectivity to this port.
49152 thru 65535	TCP/UDP	Open	MAC	no	MAC is a proprietary management protocol between the Control Station and Data Mover. It is only used on the private network between the two. This is a core process and cannot be stopped.

J.10.2 Control Station

Table J.10.2.1 Ports - Control Station

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
22	TCP	Open	SSH	Yes (Strongly not	SSH is default method of getting a shell in order to use the Control Station CLI. Telnet and other related services are not enabled by default; SSH is the recommended method of access the Control Station. Authentication is handled be the SSH daemon and uses the local user account information on the Control Station.

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
				recommended)	While this port can be closed by running the command `/sbin/sercive sshd` stop followed by `/sbin/chkconfig -del sshd`, this is not recommended.
80	TCP	Open	HTTP	No	This is the standard HTTP port. All HTTP management traffic directed to this port is automatically directed to the HTTPS port (443). No services are offered over port 80.
111	TCP/UDP	Open	rcpbind	No	The service that opens this port is the standard portmapper or rcpbind process and is auxiliary network service; it cannot be stopped. By its very nature, if a client system has network connectivity to the port, they may query it. There is no authentication performed.
161	UDP	Open	SNMP Management Infrastructure	Yes	The Simple Network management Protocol (SNMP) ia a management and monitoring service used by many third party management tools. The Control Station used SNMP, version 1 as defined by RFC 1157. This version of SNMP does not support modifying any of the monitored values. Authentication is based upon a client system knowing the community string. The community string setting is "public" by default and should be changed. Instructions on disabling the SNMP service on a Celerra Control Station are defined in the Primus solution amc44454. However, doing this will prevent auto-discovery by external management toold. If you are using ECC to monitor a Celerra, then the SNMP service must be enabled.
443	TCP	Open	HTTPS	No	This is the standard HTTPS port and is used for HTTP-based management tragic to the Control Station by both Celerra Manager and Celerra Monitor. When used by the Celerra Manager, an administrator must log in before they are granted access to the system. They are authenticated against the local Control Station administrative

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
					user accounts. Celerra Monitor has it's own authentication protocol but uses the same set of local administrative user accounts.
6389	TCP	Open	Navicli	No	CLARiiON –evr01. This port can be placed behind a firewall.
8000	TCP	Open	HTTP	Yes	This port can be used by Celerra Monitor is HTTPS is not desired for some reason. It is also used for replications commands that go between Control Stations. Celerra Monitor follows a protocol that requires all incoming traffic to be authenticated and carry a valid session token. The Control Station to Control Station replication traffic requires that an explicit trust relationship between the Control Stations be established beforehand. Then each HTTP request is cryptographically signed by then sending Control Station before being sent to the receiving Control Station. Without a valid signature, the HTTP request will not be accepted. It is not recommended that this port be disabled.
8014	TCP	Open	Java	No	This port is used for communications between the clarion agent and jserver. It is only used within the Control Station Environment (i.e. not exposed to the network).
8712	TCP	Open	NBS	No	This is used by the NBS service for access to the Control Station file system on NS-series Celerras. It is restricted to the private network between the Control Station and Data Mover.
9823	TCP	Open	nas_mcd	No	This port is used for the two nas_mcd processed to communicate with each other. It is used in two instances: 1. A standby CD "asks" the primary CD to port

Port	Protocol	Default State	Service	Can the Port Be Closed by Stopping Associated Service?	Comments
					events for it using port 9823 over the internal network. 2. In a Celerra SRDF configuration the R1 and the R2 Control Stations communicate over the IP network using port 9823. The Master Control Daemon (MCD) functions as a monitor over the system, similar to a Unix INIT process but with a NAS focus and NAS specific functionality. While the port is strictly for communication between nas_mcd process and provides a very limited interface, no additional authentication is performed (as with standard auxiliary network services).
32768	TCP/UDP	Open	statd	Yes	This port is dynamically allocated. This port can be closed by running the command `/sbin/service nfslock stop` followed by `/sbin/chkconfig -del nfslock`
39494	TPC/UDP	Open	Lockd	Yes	The lockd daemon that works in concert with statd. This port is dynamically allocated. It is closed by running the commands mentioned in the statd section above.

J.10.3 Ports the Data Mover/Blade May Contact

The table below lists the network connections that may be initiated by the Celerra's Data Mover/Blade.

Table J.10.3.1 Ports the Data Mover/Blade May Contact

Protocol	Port	Purpose	On What Host(s)
TCP/UDP	53	DNS	All Windows 2000 and above Domain Controllers/DNS Servers
TCP/UDP	88	Kerberos Ticket	All Kerberos KDCs (Key Distribution Centers). This applies to Windows 2000 and above Domain Controllers as well as to Unix and Linux KDCs.
TCP/UDP	111	Portmapper	All NFS clients, VC Servers, and NIS servers
TCP/UDP	137	WINS	All WINS servers
UDP	138	NETBIOS Datagram Service	All CIFS clients (used for notification and popups)
TCP	139	CIFS (on Domain Controllers)	All Windows NT Domain Controllers
UDP	161	SNMP	All hosts to which the Data Mover will send SNMP traps
TCP/UDP	389	LDAP	All Windows 2000 and above Domain Controllers or other LDAP Servers
UDP	3268	LDAP	Queries to the Windows 2000 and above General Catalog
TCP	445	CIFS (on domain controller)	All Windows Domain Controllers
TCP/UDP	464	Kerberos Password	All Windows 2000 and above Domain Controllers or other KPASSWD servers
TCP/UDP	625	FMP	Windows WPFS clients

Protocol	Port	Purpose	On What Host(s)
TCP/UDP	6907	FMP	Unix FPMS clients
TCP/UDP	Dynamic	Lockd	All NFS clients
TCP/UDP	Dynamic	Statd	All NFS clients
TCP/UDP	Dynamic	NIS	NIS servers

J.10.4 Celerra Default Accounts

Table J.10.4.1 Celerra Default Accounts

User Account	Description
Root	Similar to a traditional UNIX machine, the root user (or superuser) is the first user account created when Celerra is initially installed. The roos user could be considered as the System Administrator of the Control Station/Celerra and has the Ability to perform system administrator tasks.
Nasadmin	The nasadmin user is created as the default Celerra administrator when a Celerra is installed in the factory. If the Celerra software is installed on site a default account is created, but the name of the account may be modified at the discretion of the installer. Nasadmin has the ability to perform a majority of the Celerra administrative tasks. The remaining tasks require root privileges.

Nore: Additional Accounts exist on the Control Station, but these are the only two that can be logged into.

J.10.5 Ports Centera

Table J.10.5 Ports - Centera

Component	Service	Protocol	Port	Description

Component	Service	Protocol	Port	Description
CentraStar	SSH (Unlocked Nodes only)	TCP	22	Incoming and replies
CentraStar	SHCP (if configured)	UDP	67-68	Outgoing and replies
CentraStar	DHCP (in configured)	Broadcast	67-68	Incoming
CentraStar	DNS (if configured)	TCP/UDP	53	Outgoing and replies
CentraStar	SMTP (if configured)	TCP	25	Outgoing and replies
CentraStar	SNMP Trap (if configured)	UDP	162	Outgoing
CentraStar	SNMP Get request (if configured)	UDP	1610	Incoming and replies
CentraStar	ICMP	ICMP		Outgoing and Replies
CentraStar	Syslog (if configured)	UDP	514	Outgoing
CentraStar	Smartpockets	TCP/UDP	3218	Incoming/Outgoing
CentraStar	Centera Management Protocol	TCP/UDP	3682	Incoming/Outgoing
CentraStar	Centera Federations	TCP/UDP	3220	Incoming/Outgoing
CentraStar	FTP	TCP	21	Outgoing